УТВЕРЖДЕНО
Правлением Союза
(Протокол №44 от 03.12.2018 г.)

ОДОБРЕНО
Решением Экспертного совета
при Союзе «Агентство развития
профессиональных сообществ
и рабочих кадров
«Молодые профессионалы
(Ворлдскиллс Россия)»
(Протокол №18/11 от 12.11.2018 г.)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА ПО СТАНДАРТАМ ВОРЛДСКИЛЛС РОССИЯ ПО КОМПЕТЕНЦИИ «СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ» В 2019 ГОДУ

СОДЕРЖАНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к Оценочным материалам для демонстрационного экзамена по стандартам Ворлдскиллс Россия по компетенции «Сетевое и системное администрирование»
(далее – Оценочные материалы)

Оценочные материалы разработаны экспертным сообществом Ворлдскиллс в целях организации и проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия по компетенции «Сетевое и системное администрирование».

Оценочные материалы содержат комплекты оценочной документации (далее – КОД):

● КОД № 2.1 - комплект, предусматривающий задание с максимально возможным баллом 75 для оценки знаний, умений и навыков по всем разделам Спецификации стандарта компетенции «Сетевое и системное администрирование» и продолжительностью 10,5 часов.

● КОД № 1.1 - комплект с максимально возможным баллом 45 и продолжительностью 6 часов, предусматривающий задание для оценки знаний, умений и навыков по минимальным требованиям Спецификации стандарта компетенции «Сетевое и системное администрирование».

Каждый КОД содержит:

● Паспорт КОД с указанием:

а) перечня знаний, умений и навыков из Спецификации стандарта компетенции «Сетевое и системное администрирование», проверяемых в рамках КОД;

б) обобщенной оценочной ведомости;

в) количества экспертов, участвующих в оценке выполнения задания;

г) списка оборудования и материалов, запрещенных на площадке (при наличии);

Инструкцию по охране труда и технике безопасности для проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия;

Образец задания для демонстрационного экзамена по стандартам Ворлдскиллс Россия;

Инфраструктурный лист;

План проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия с указанием времени и продолжительности работы участников и экспертов;

План застройки площадки для проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия.

ИНСТРУКЦИЯ ПО ОХРАНЕ ТРУДА И ТЕХНИКЕ БЕЗОПАСНОСТИ
для проведения демонстрационного экзамена
по стандартам Ворлдскиллс Россия по компетенции:
«Сетевое и системное администрирование»

1. Общие требования охраны труда

1.1. К самостоятельной работе с ПК допускаются участники после прохождения ими инструктажа на рабочем месте, обучения безопасным методам работ и проверки знаний по охране труда, прошедшие медицинское освидетельствование на предмет установления противопоказаний к работе с компьютером.

1.2. При работе с ПК рекомендуется организация перерывов на 10 минут через каждые 50 минут работы. Время на перерывы уже учтено в общем времени задания, и дополнительное время участникам не предоставляется.

1.3. При работе на ПК могут воздействовать опасные и вредные производственные факторы:

– физические: повышенный уровень электромагнитного излучения; повышенный уровень статического электричества; повышенная яркость светового изображения; повышенный уровень пульсации светового потока; повышенное значение напряжения в электрической цепи, замыкание которой может произойти через тело человека; повышенный или пониженный уровень освещенности; повышенный уровень прямой и отраженной блесткости;

– психофизиологические: напряжение зрения и внимания; интеллектуальные и эмоциональные нагрузки; длительные статические нагрузки; монотонность труда.

1.4. Запрещается находиться возле ПК в верхней одежде, принимать пищу и курить, употреблять во время работы алкогольные напитки, а также быть в состоянии алкогольного, наркотического или другого опьянения.

1.5. Участник соревнования должен знать месторасположение первичных средств пожаротушения и уметь ими пользоваться.

1.6. О каждом несчастном случае пострадавший или очевидец несчастного случая немедленно должен известить ближайшего эксперта.

1.7. Участник соревнования должен знать местонахождения медицинской аптечки, правильно пользоваться медикаментами; знать инструкцию по оказанию первой медицинской помощи пострадавшим и уметь оказать медицинскую помощь. При необходимости вызвать скорую медицинскую помощь или доставить в медицинское учреждение.

1.8. При работе с ПК участник соревнования должны соблюдать правила личной гигиены.

1.9. Работа на конкурсной площадке разрешается исключительно в присутствии эксперта. Запрещается присутствие на конкурсной площадке посторонних лиц.

1.10. По всем вопросам, связанным с работой компьютера следует обращаться к руководителю.

1.11. За невыполнение данной инструкции виновные привлекаются к ответственности согласно правилам внутреннего распорядка или взысканиям, определенным Кодексом законов о труде Российской Федерации.

2. Требования охраны труда перед началом работы

2.1. Перед включением используемого на рабочем месте оборудования участник соревнования обязан:

2.1.1. Осмотреть и привести в порядок рабочее место, убрать все посторонние предметы, которые могут отвлекать внимание и затруднять работу.

2.1.2. Проверить правильность установки стола, стула, подставки под ноги, угол наклона экрана монитора, положения клавиатуры в целях исключения неудобных поз и длительных напряжений тела. Особо обратить внимание на то, что дисплей должен находиться на расстоянии не менее 50 см от глаз (оптимально 60-70 см).

2.1.3. Проверить правильность расположения оборудования.

2.1.4. Кабели электропитания, удлинители, сетевые фильтры должны находиться с тыльной стороны рабочего места.

2.1.5. Убедиться в отсутствии засветок, отражений и бликов на экране монитора.

2.1.6. Убедиться в том, что на устройствах ПК (системный блок, монитор, клавиатура) не располагаются сосуды с жидкостями, сыпучими материалами (чай, кофе, сок, вода и пр.).

2.1.7. Включить электропитание в последовательности, установленной инструкцией по эксплуатации на оборудование; убедиться в правильном выполнении процедуры загрузки оборудования, правильных настройках.

2.2. При выявлении неполадок сообщить об этом эксперту и до их устранения к работе не приступать.

3. Требования охраны труда во время работы

3.1. В течение всего времени работы со средствами компьютерной и оргтехники участник соревнования обязан:

- содержать в порядке и чистоте рабочее место;
- следить за тем, чтобы вентиляционные отверстия устройств ничем не были закрыты;
- выполнять требования инструкции по эксплуатации оборудования;
- соблюдать, установленные расписанием, трудовым распорядком регламентированные перерывы в работе, выполнять рекомендованные физические упражнения.

3.2. Студенту запрещается во время работы:

- отключать и подключать интерфейсные кабели периферийных устройств;
- класть на устройства средств компьютерной и оргтехники бумаги, папки и прочие посторонние предметы;
- прикасаться к задней панели системного блока (процессора) при включенном питании;
- отключать электропитание во время выполнения программы, процесса;
- допускать попадание влаги, грязи, сыпучих веществ на устройства средств компьютерной и оргтехники;
- производить самостоятельно вскрытие и ремонт оборудования;
- производить самостоятельно вскрытие и заправку картриджей принтеров или копиров;
- работать со снятыми кожухами устройств компьютерной и оргтехники;
- располагаться при работе на расстоянии менее 50 см от экрана монитора.

3.3. При работе с текстами на бумаге, листы надо располагать как можно ближе к экрану, чтобы избежать частых движений головой и глазами при переводе взгляда.

3.4. Рабочие столы следует размещать таким образом, чтобы видеодисплейные терминалы были ориентированы боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева.

3.5. Освещение не должно создавать бликов на поверхности экрана.

3.6. Продолжительность работы на ПК без регламентированных перерывов не должна превышать 1-го часа. Во время регламентированного перерыва с целью снижения нервно-эмоционального напряжения, утомления зрительного аппарата, необходимо выполнять комплексы физических упражнений.

4. Требования охраны труда в аварийных ситуациях

4.1. Обо всех неисправностях в работе оборудования и аварийных ситуациях сообщать непосредственно эксперту.

4.2. При обнаружении обрыва проводов питания или нарушения целостности их изоляции, неисправности заземления и других повреждений электрооборудования, появления запаха гари, посторонних звуков в работе оборудования и тестовых сигналов, немедленно прекратить работу и отключить питание.

4.3. При поражении пользователя электрическим током принять меры по его освобождению от действия тока путем отключения электропитания и до прибытия врача оказать потерпевшему первую медицинскую помощь.

4.4. В случае возгорания оборудования отключить питание, сообщить эксперту, позвонить в пожарную охрану, после чего приступить к тушению пожара имеющимися средствами.

5. Требования охраны труда по окончании работы

5.1. По окончании работы участник соревнования обязан соблюдать следующую последовательность отключения оборудования:

- произвести завершение всех выполняемых на ПК задач;
- отключить питание в последовательности, установленной инструкцией по эксплуатации данного оборудования.
- В любом случае следовать указаниям экспертов

5.2. Убрать со стола рабочие материалы и привести в порядок рабочее место.

5.3. Обо всех замеченных неполадках сообщить эксперту.

1. КОМПЛЕКТ ОЦЕНОЧНОЙ ДОКУМЕНТАЦИИ № 2.1
для демонстрационного экзамена
по стандартам Ворлдскиллс Россия
по компетенции
«Сетевое и системное администрирование»

1.1. Паспорт Комплекта оценочной документации № 2.1

КОД 2.1 по компетенции «Сетевое и системное администрирование»

разработан в целях организации и проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия по *код и наименование профессии и/или специальности среднего профессионального образования, по которому (ым) проводится демонстрационный экзамен*

(из перечня профессий среднего профессионального образования и перечня специальностей среднего профессионального образования, утвержденных приказом Министерства образования и науки Российской Федерации от 29 октября 2013 года №1199).

1. Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта компетенции «Сетевое и системное администрирование» (WorldSkills Standards Specifications, WSSS), проверяемый в рамках комплекта оценочной документации

	Раздел WSSS
3	**Консультирование и поддержка пользователей** Участник должен знать и понимать: Основные возможности определенного круга ИТ-систем для обеспечения качественной поддержки; Подходы к планированию рабочего процесса с целью обеспечения высокого уровня обслуживания, способного удовлетворить потребности пользователя и организации; Различные методы демонстрации и презентации для поддержки развития навыков и знаний пользователя; Различные методы оценки возможностей пользователя с целью удовлетворения его немедленных потребностей и поощрения к саморазвитию; Различные методики обучения, позволяющие адаптировать процесс обучения с учетом навыков и возможностей пользователей; Тренды и вызовы современной IT-индустрии и способы развития, которые могут быть представлены пользователям; Способы ведения переговоров для различных ситуаций. Участник должен уметь: Заблаговременно поддерживать уровень собственных познаний в сфере информационных технологий; Своевременно (в установленных регламентом рамках) отвечать на запросы как локальных, так и удаленных пользователей; Планировать и постоянно актуализировать планы выполнения пользовательских запросов к поддержке для балансировки

	потребностей пользователей и организации; Точно определять требования пользователя и оправдывать ожидания; Подсчитывать время и стоимость выполнения работы; Выбирать наиболее подходящие способы демонстрации для более точного соответствия подачи материала навыкам и знания аудитории; Эффективно демонстрировать информационные системы пользователям и группам пользователей для предоставления им возможностей к улучшению своих навыков и знаний; Успешно обучать пользователей очно и заочно для успешного разрешения проблем в области ИТ-инфраструктуры, представления новых продуктов, улучшения пользовательских навыков и знаний; Определять возможности к улучшению продукта и общей удовлетворенности пользователя; Формировать точные, своевременные рекомендации в области обновления и приобретения новых IT-продуктов и сервисов для улучшения качества принятия решений; Формировать корректные, отвечающие требованиям и ограничениям, рекомендации на основе запросов и потребностей; Принимать участие в тендерных и закупочных процедурах
4	**Поиск и устранение неисправностей** Участник 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. Участник 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
6	**Настройка, обновление и конфигурация операционных систем** Участник 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. Участник 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**

	Участник должен знать и понимать: Сетевое окружение; Сетевые протоколы; Процесс построения сети и как сетевые устройства могут быть настроены для эффективного взаимодействия; Типы сетевых устройств. Участник 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. Обобщенная оценочная ведомость

В данном разделе определяются критерии оценки и количество начисляемых баллов (субъективные и объективные)

Общее количество баллов задания/модуля по всем критериям оценки составляет 75.

Раздел	**Критерий**	**Оценки**		
		Судейство	**Объективная**	**Общая**
WSSS Sec.6	Расширенная настройка ОС Linux	0	23	23
WSSS Sec.6	Расширенная настройка ОС Windows	0	23	23
WSSS Sec. 7	Расширенные сетевые технологии	0	23	23
WSSS Sec 3, 4	Расширенная настройка ОС Linux Расширенная настройка ОС Windows Расширенные сетевые технологии	0	6	6
Итого =		0	75	75

3. Количество экспертов, участвующих в оценке выполнения задания

3.1. Минимальное количество экспертов, участвующих в оценке демонстрационного экзамена по стандартам Ворлдскиллс Россия по компетенции «Сетевое и системное администрирование» - 3 чел.

Количество постов-рабочих мест / Количество студентов	1 до 5	6 до 10	11 до 15	16 до 20	21 до 25	26 и более
От 1 до 5	3					
От 6 до 10		3				
От 11 до 15			3			
От 16 до 20				6		
От 21 до 25					9	
От 26 и более						9

3.2. Дополнительное количество экспертов рассчитывается исходя из количества участников демонстрационного экзамена.

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

В соответствии с ИЛ

Инфраструктурный лист для КОД № 2.1 – приложение №1

1.2. Задание для демонстрационного экзамена по стандартам Ворлдскиллс Россия по компетенции «Сетевое и системное администрирование» (образец)

Задание включает в себя следующие разделы:

- Формы участия
- Модули задания и необходимое время
- Критерии оценки
- Необходимые приложения

Количество часов на выполнение задания: 10,5 ч.

1. ФОРМА УЧАСТИЯ

индивидуальная

2. МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ

Модули и время сведены в таблице 1
Таблица 1.

№ п/п	Наименование модуля	Максимальный балл	Время на выполнение
1	Модуль A - Расширенная настройка Linux	25	3,5 часа
2	Модуль B - Расширенная настройка Windows	25	3,5 часа
3	Модуль C – Расширенные сетевые технологии	25	3,5 часа

Модули с описанием работ

Модуль 1: Модуль A - Расширенная настройка Linux

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/**

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.

5) 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

6) 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

7) 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.**

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

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

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

        iii. Скрипты должны вызываться из любого каталога без указания пути

    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.

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**

   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

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

2) 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

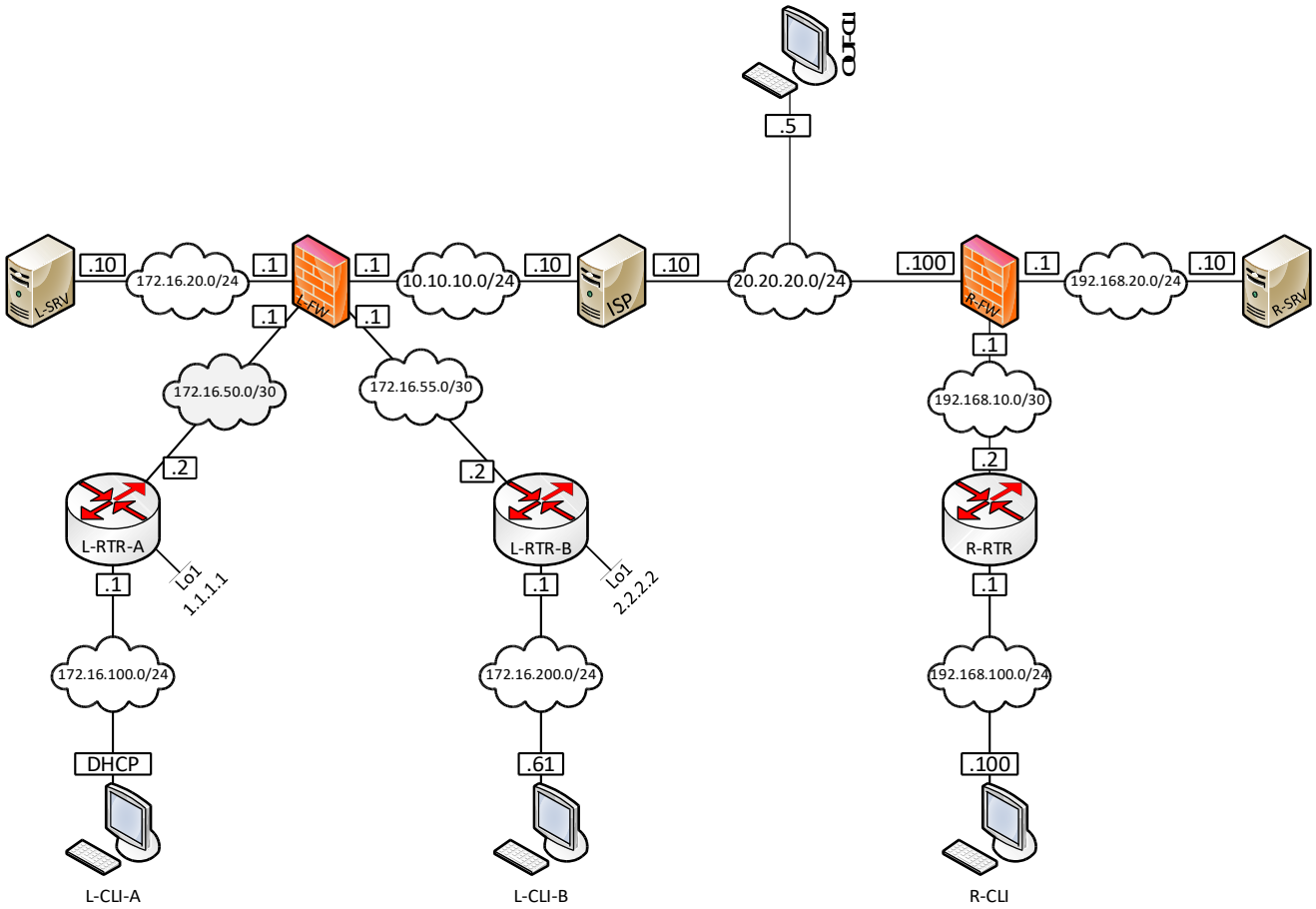
Таблица 3 – Правила журналирования

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

3) *<HOSTNAME> - название директории для журналируемого хоста

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

ДИАГРАММА ВИРТУАЛЬНОЙ СЕТИ



Модуль 2: Модуль B - Базовая настройка Windows

Настройка DC-M

Базовая настройка

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

Active Directory

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

DHCP

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

DNS

- настройте необходимые зоны прямого и обратного просмотра, обеспечьте их согласованную работу со службой DNS на FILES-M;
- создайте вручную все необходимые записи типа A и PTR для серверов домена и необходимых web-сервисов;
- 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

- запретите анимацию при первом входе пользователей в систему на всех клиентских компьютерах домена;
- члены группы IT должны быть членами группы локальных администраторов на всех клиентских компьютерах домена;

- в браузерах IE Explorer и Microsoft Edge (установите и используйте windows10.admx) должна быть настроена стартовая страница – www.moscow.ru;
- запретите изменение экранной заставки и *Корзину* на рабочем столе для всех пользователей домена, кроме членов группы локальных администраторов клиентских компьютеров;
- для членов группы Experts настройте перенаправление папок *my Documents* и *Desktop* по адресу FILES-M→d:\shares\redirected.

Элементы доменной инфраструктуры

- создайте подразделения: Experts, Competitors, Managers, Visitors, IT и Project;
- 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;

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.

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

Настройка FILES-M

Базовая настройка

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

- присоедините компьютер к домену Moscow.ru;
- из четырех имеющихся жестких дисков создайте RAID-5 массив; назначьте ему букву D:\.

Active Directory

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

DHCP

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

DNS

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

Общие папки

- создайте общие папки для подразделений (Competitors, Experts and Managers) по адресу FILES-M→d:\shares\departments;
- обеспечьте привязку общей папки подразделения к соответствующей группе в качестве диска G:\;
- создайте общую папку проектов по адресу FILES-M→d:\shares\projects;
- в папке d:\shares\projects создайте следующие папки: Budget, Intranet, Logistics; настройте разрешения этих папок в соответствии с таблицей 2;
- 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

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

IIS

- создайте сайт для менеджеров компании (используйте предоставленный htm-файл в качестве документа по умолчанию);

Настройка ROOTCA-M

Базовая настройка

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

Службы сертификации

- установите службы сертификации;
- настройте одиночный корневой сервер сертификации (длина ключа и алгоритмы шифрования значения не имеют);
- имя центра сертификации – Moscow Root CA;
- срок действия сертификата – 10 лет;
- CRL location: http://SUBCA-M.Moscow.ru/certenroll/<caname><crlnamesuffix><deltacrlallowed>.crl
- AIA location: http://SUBCA-M.Moscow.ru/certenroll/<serverdnsname>_<caname><certificatename>.crt
- создайте список отзыва сертификатов и сертификат корневого центра сертификации для SUBCA-M;
- выпустите сертификат подчиненного центра сертификации для SUBCA-M, одобрив соответствующий запрос;
- после всех настроек отключите сетевой интерфейс.

Настройка SUBCA-M

Базовая настройка

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

Службы сертификации

- установите службы сертификации;

- настройте подчиненный доменный центр сертификации;
- имя центра сертификации – Moscow Sub CA;
- срок действия сертификата – 5 лет;
- импортируйте и опубликуйте список отзыва сертификатов с ROOTCA-M;
- настройте шаблон выдаваемого сертификата для клиентских компьютеров *MoscowClients*: *subject name=common name*, автозапрос для всех клиентских компьютеров домена;

Настройка CLIENT-M

Базовая настройка

- переименуйте компьютер в CLIENT-M;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к домену Moscow.ru;
- установите набор компонентов удаленного администрирования RSAT;
- запретите использование «спящего режима»;
- 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

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

DNS

- 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);
- обеспечьте разрешение имен сайтов www.moscow.ru и www.izhevsk.ru.

Работа с IIS-IZ

IIS

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

Работа с CLIENT-IZ

Базовая настройка

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

Настройка INET

Базовая настройка

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

DNS/IIS

- настройте эмуляцию подключения к Интернету, принимая во внимание версии используемых операционных систем;
- 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

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

Настройка EDGE-IZ

Базовая настройка

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

Настройка RRAS

- установите службу RRAS;
- 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;
- 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

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

Настройка RRAS

- установите службу RRAS;
- 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 Direct Access

- сделайте учетные записи компьютеров CLIENT-M и REMOTE-M членам группы DAClients;
- только члены группы DAClients могут подключаться к сети с использованием Direct Access;
- название соединения – *DA-Moscow*;

- в качестве NCA используйте FILES-M;
- для подключения внешних клиентов используйте имя *connect.moscow.ru*;
- для настройки используйте соответствующий сертификат, выданный SUBCA-M (использование самозаверенных сертификатов не допускается);
- клиенты Direct Access должны иметь полный доступ к общим ресурсам в обоих офисах.

Настройка REMOTE-M

Базовая настройка

- переименуйте компьютер в REMOTE-M;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- запретите использование «спящего режима»;
- не меняя сетевых настроек (сетевой интерфейс должен быть соединен с сетью Internet) присоедините компьютер к домену Moscow.ru в режиме OFFLINE;
- сохраните созданный на DC-M файл ответов для offline-присоединения к домену по адресу C:\Remote.txt.

Таблица 1 – Реквизиты

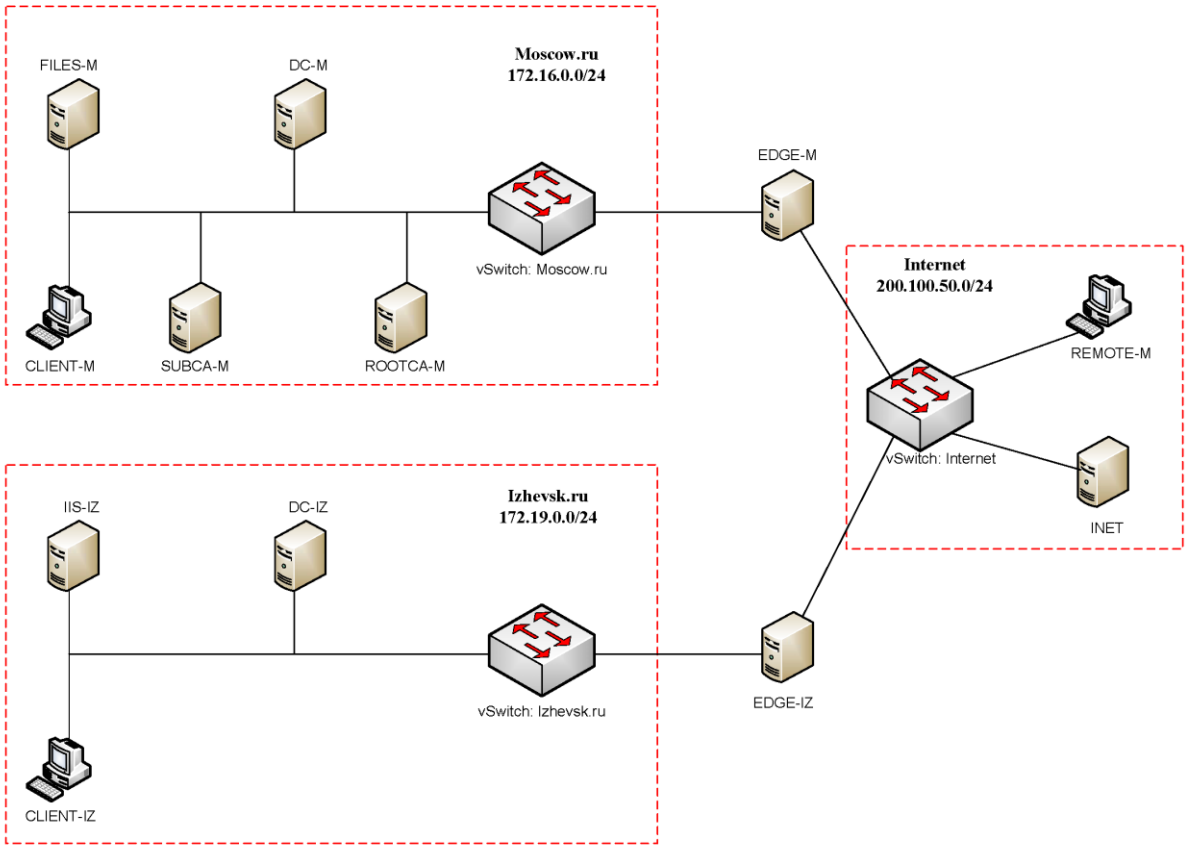
Имя компьютера	Имя домена	IP-адреса
DC-IZ	Izhevsk.ru	172.19.0.1/24
CLIENT-IZ		DHCP
IIS-IZ		172.19.0.3/24
EDGE-IZ		172.19.0.250/24 200.100.50.101/24
DC-M	Moscow.ru	172.16.0.1/24
FILES-M		172.16.0.2/24
SUBCA-M		172.16.0.4/24
EDGE-M		172.16.0.250/24 200.100.50.100/24
CLIENT-M		DHCP
REMOTE-M		DHCP

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

ДИАГРАММА ВИРТУАЛЬНОЙ СЕТИ



Модуль 3: Модуль С – Базовые сетевые технологии

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

B. 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. Все агрегированные каналы должны работать в режиме L2.
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 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.

C. 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 10.1.1.1 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 (11.11.11.11/32) 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 с помощью связки ключей **EIGRP** с ключом **WSR** и номером ключа **2**.

c. Провайдер ISP1 выполняет редистрибуцию маршрута 11.11.11.11/32 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
BR2	65020

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 маршрута по умолчанию из BGP в OSPF. Все устройства должны предпочитать маршрут от HQ1, и переключаться на маршрут через ASA только в случае отсутствия связи на HQ1.

D. 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 1.1.1.1.
   b. На маршрутизаторе BR1 настройте динамическую трансляцию портов (PAT) для сети 192.168.1.0/24 в адрес петлевого интерфейса 11.11.11.11.
   c. На маршрутизаторе BR2 настройте динамическую трансляцию портов (PAT) для сети 192.168.2.0/24 в адрес петлевого интерфейса 22.22.22.22.

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.

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

    f. 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.

F. Настройка параметров мониторинга и резервного копирования

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

H. 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.

I. 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

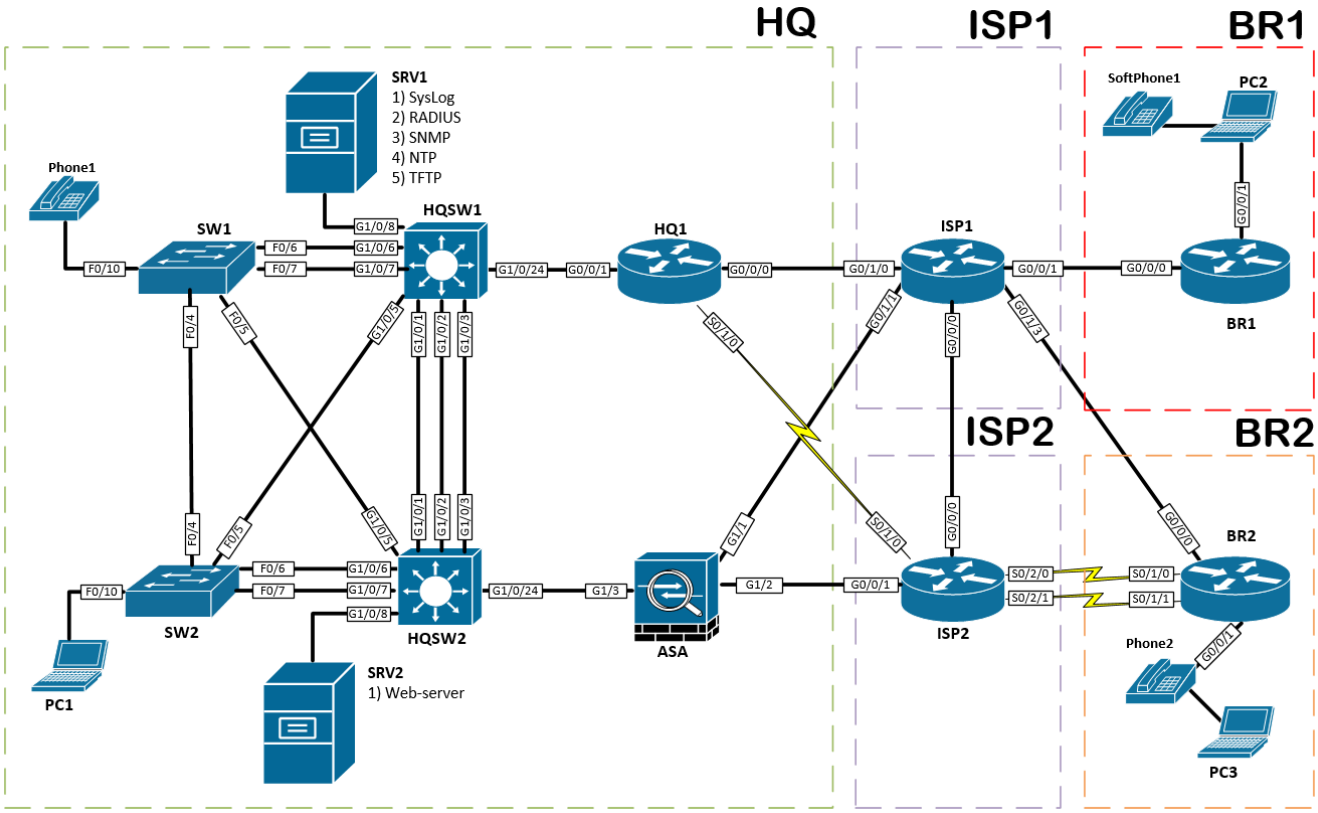
Для названия

J. Конфигурация виртуальных частных сетей

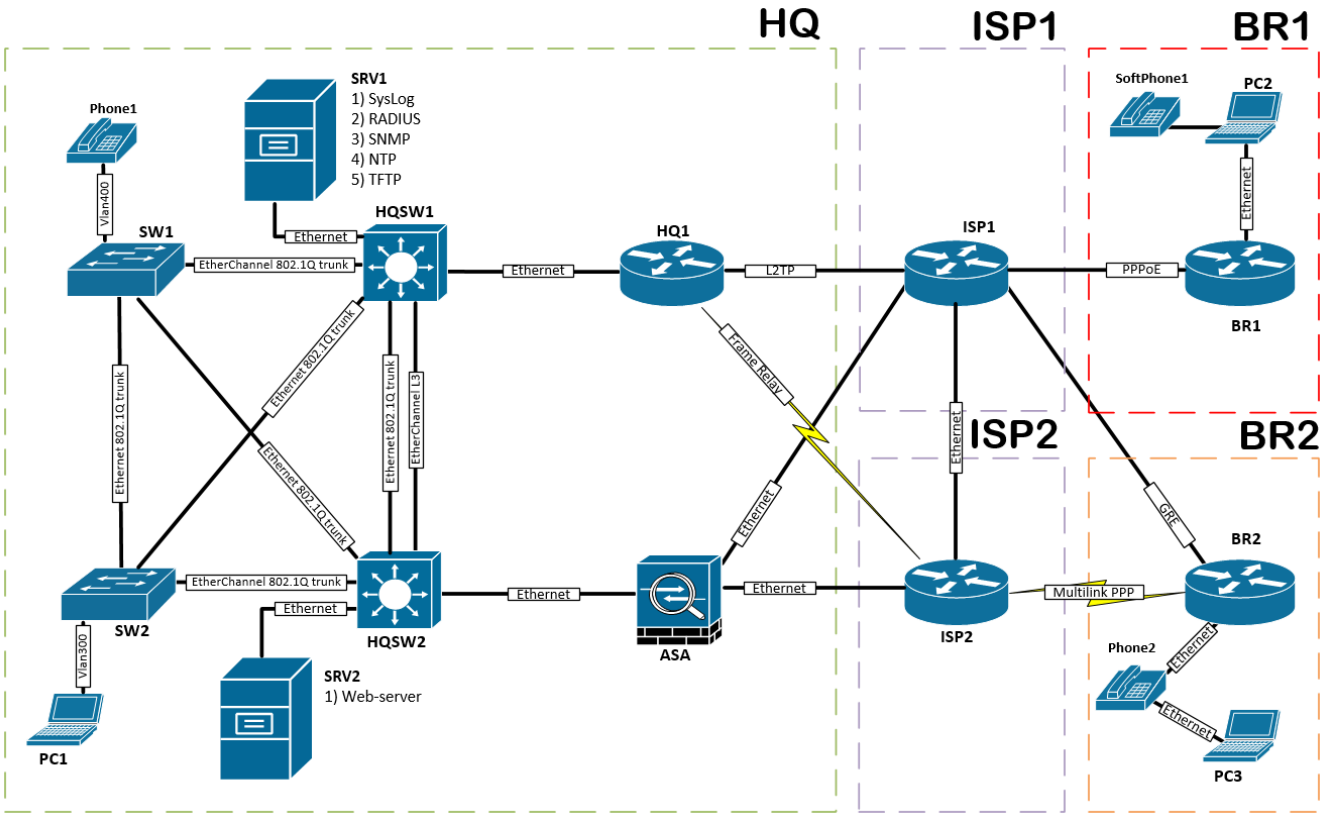
1. На маршрутизаторах HQ1, BR1 и BR2 настройте DMVPN:
    a. Используйте в качестве VTI интерфейс Tunnel1
    b. На каждом интерфейсе установите значение MTU равное 1400 для IPv4 и IPv6.
    c. Используйте адресацию в соответствии с VPN-диаграммой
    d. Режим — GRE Multipoint
    e. Интерфейс-источник — 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
    b. Параметры преобразования трафика для второй фазы:
        i. Протокол – ESP
        ii. Шифрование – AES

Проверка целостности – MD5

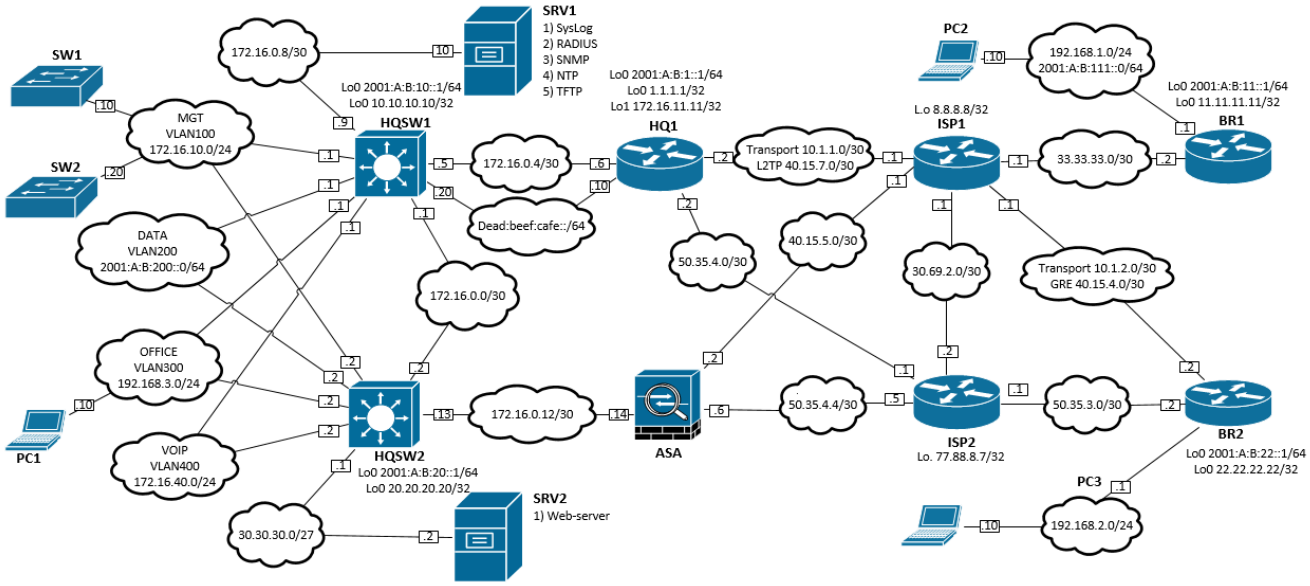
Топология L1



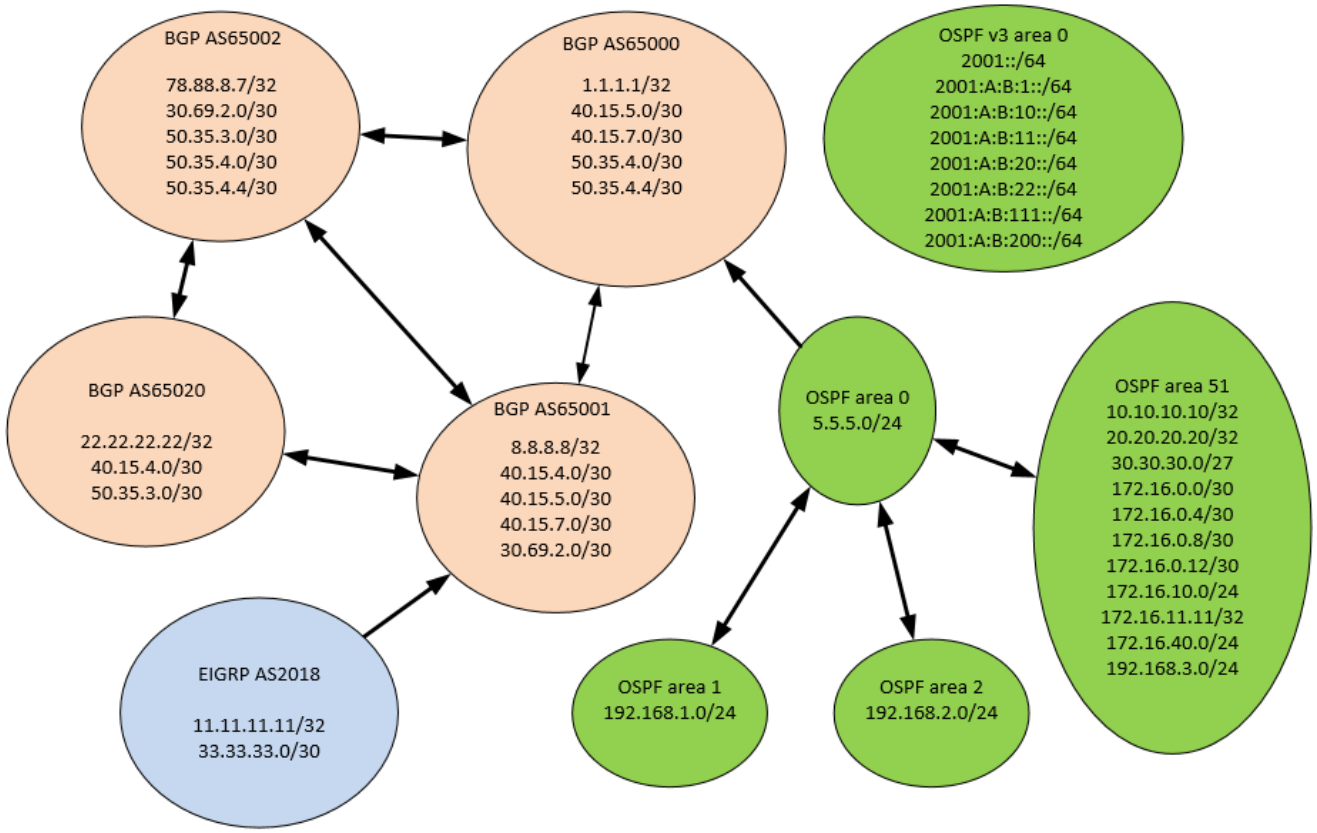
Топология L2



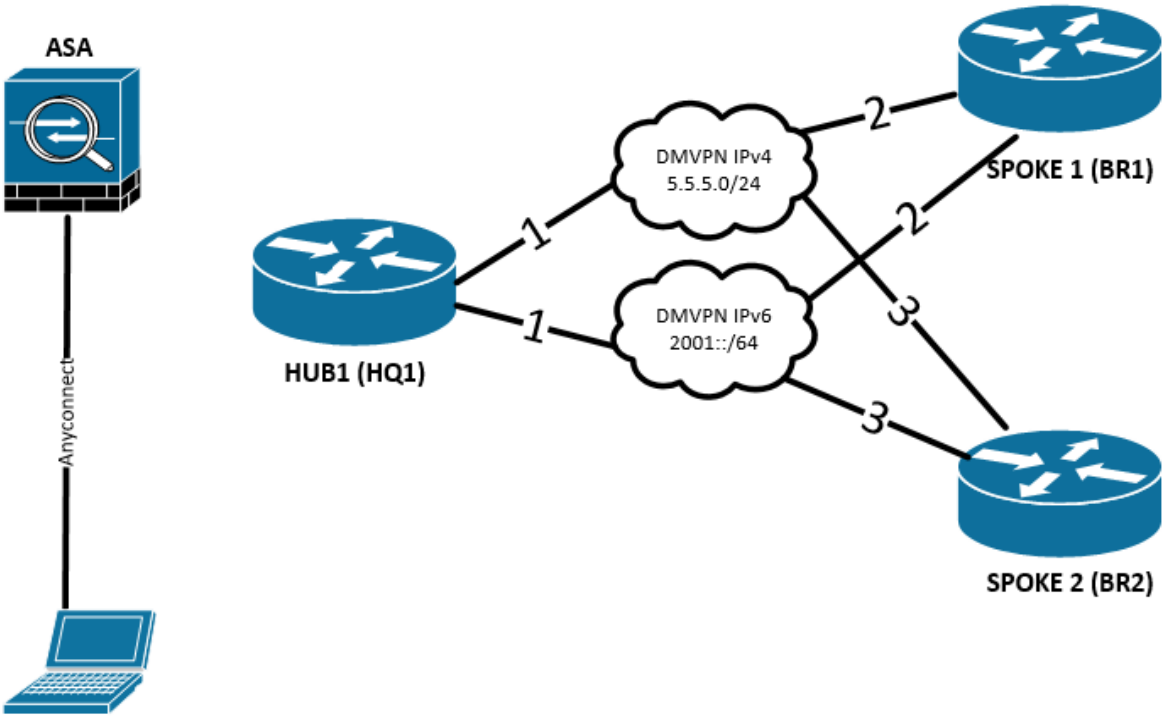
Топология L3



Routing-диаграмма



VPN диаграмма



3. КРИТЕРИИ ОЦЕНКИ

В данном разделе определены критерии оценки и количество начисляемых баллов (субъективные и объективные) в Таблице 2.

Общее количество баллов задания/модуля по всем критериям оценки составляет 75.

Таблица 2.

Раздел	**Критерий**	**Оценки**		
		Судейство	**Объективная**	**Общая**
WSSS Sec.6	Расширенная настройка ОС Linux	0	23	23
WSSS Sec.6	Расширенная настройка ОС Windows	0	23	23
WSSS Sec. 7	Расширенные сетевые технологии	0	23	23
WSSS Sec 3, 4	Расширенная настройка ОС Linux Расширенная настройка ОС Windows Расширенные сетевые технологии	0	6	6
Итого =		0	75	75

Субъективные оценки -0.

4. НЕОБХОДИМЫЕ ПРИЛОЖЕНИЯ

Нет.

1.3. План проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия

Данное задание рассчитано на 1 день или 8 часов. План экзамена будет структурирован следующим образом:

За два дня до экзамена должно быть полностью готово оборудование. В этот же день необходимо провести собрание экспертов, на котором пройти необходимый инструктаж. Эксперты должны чётко понимать свои роли и функции, а также планируемый график работы.

За день до экзамена необходимо зарегистрировать участников, проверить паспорта и провести для них необходимый инструктаж. После прохождения инструктажа по технике безопасности и охране труда участники могут приступить к ознакомлению с рабочими местами. Рекомендуется выделить не менее 30 минут на каждый из модулей. По завершению ознакомления технический эксперт должен вернуть рабочие места к исходному состоянию и убедиться, что всё готово к началу экзамена.

В днь проведения экзамена проводится краткий брифинг и жеребьёвка по рабочим местам. В первый день при жеребьёвке определяется порядок выполнения модулей (Linux – Windows – Cisco, Windows – Cisco – Linux, Cisco – Linux – Windows) и номер рабочего места в этот день. После этого участники приступают к выполнению одного из модулей A, B и C – согласно жеребьёвке. На модуль отводится 2 часа. Завершая выполнение этого модуля, участники уходят на обед. После обеда участники приступают к выполнению следующего модуля.

Проверка выполнения задания начинается после завершения выполнения всех модулей. Начать проверку раньше не следует. Проверка организуется параллельно с выполнением в отдельном помещении.

План проведения демонстрационного экзамена корректируется главным экспертом площадки проведения демонстрационного экзамена в зависимости от времени, выделенного на площадке проведения демонстрационного экзамена, количества участников и рабочих мест.

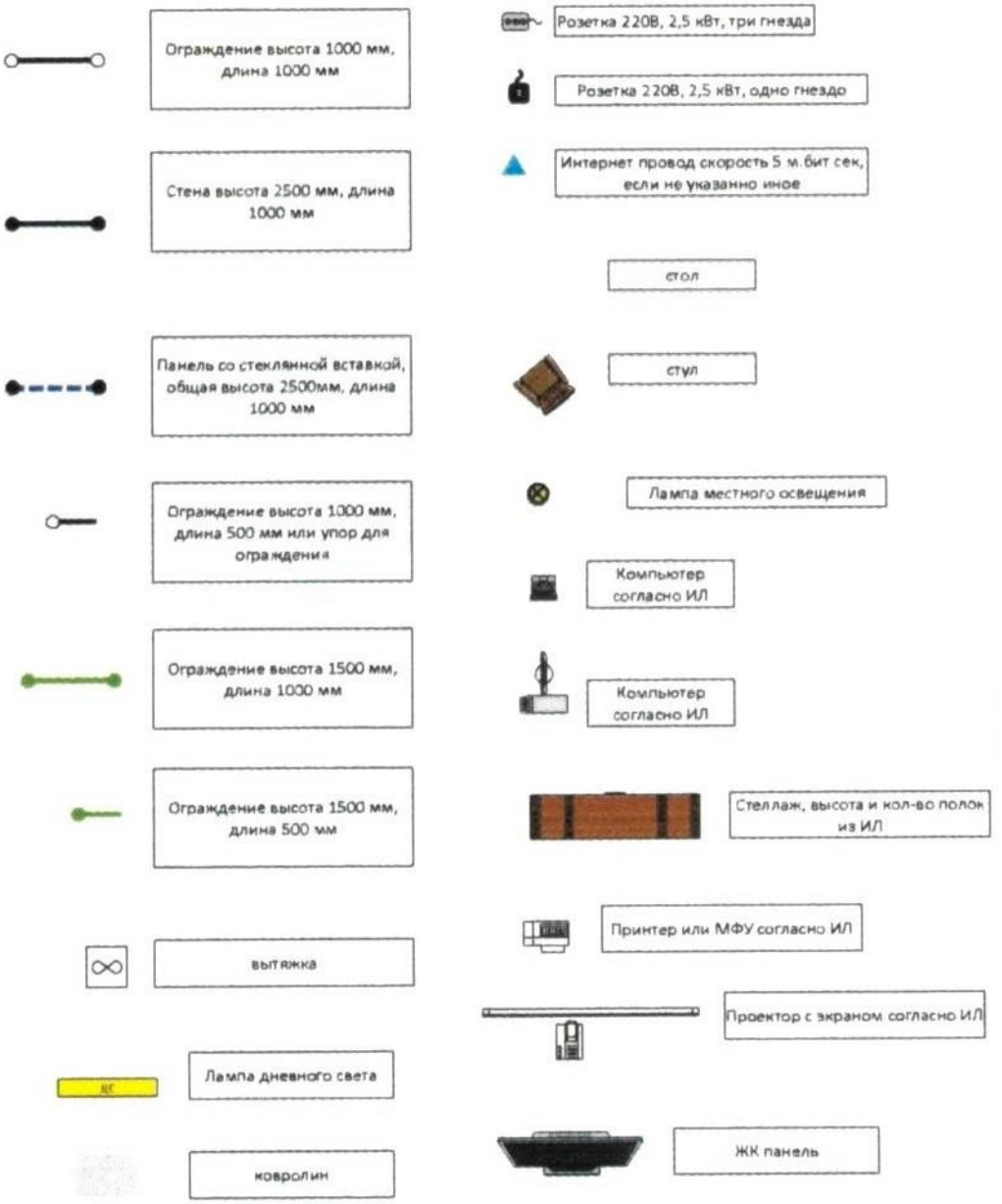
Пример плана проведения:

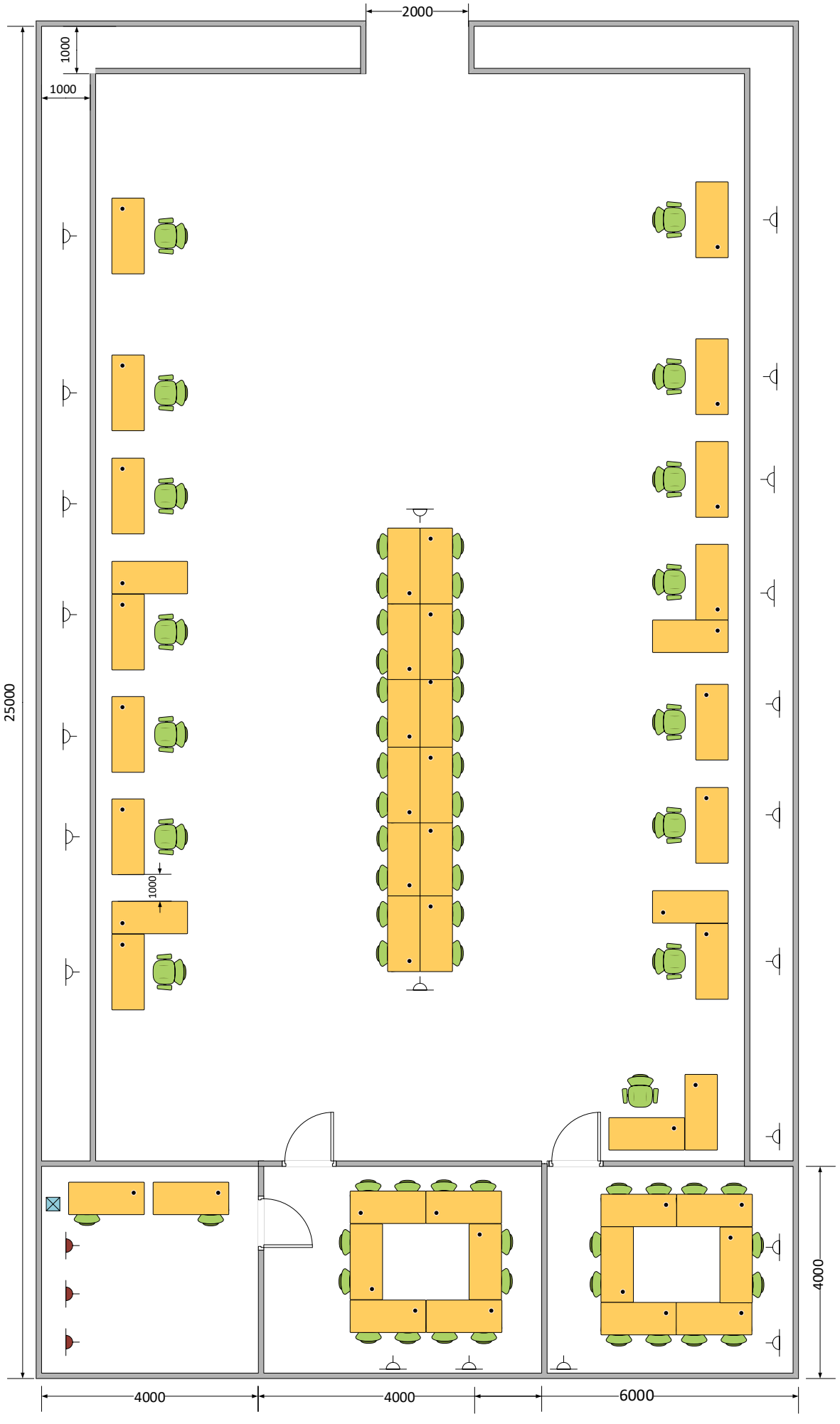
день	С-2	С-1	С1	С2	С+1
дата					
описание	Подготовительные дни		Дни экзамена		Отъезд

С-2	
время	**план мероприятия**
09:00-18:00	Завершение застройки и монтажа мебели, оргтехники, стендов и оборудования
09:00-18:00	Приезд экспертов
18:00-19:00	Собрание экспертов. Инструктаж. Распределение ролей и формирование групп оценки.
С-1	
время	**план мероприятия**
13:00-13:30	Регистрация участников на конкурсной площадке
13:30-14:00	Инструктаж участников по ОТ и ТБ
14:00-16:00	Ознакомление с рабочими местами и оборудованием.
16:00-18:00	Подготовка конкурсных мест. Проверка оборудования.
С1	
время	**план мероприятия**
08:00-08:30	Сбор участников и экспертов на площадке
08:30-09:00	Брифинг для участников, жеребьевка
09:00-12:30	**Выполнение задания (Модули A/B/C)**
12:30-13:00	Обеденный перерыв
13:00-16:30	**Выполнение задания (Модули A/B/C)**
16:30-21:00	Проведение оценки.
С2	
08:00-08:30	Сбор участников и экспертов на площадке
08:30-09:00	Брифинг для участников, жеребьевка
09:00-12:30	**Выполнение задания (Модули A/B/C)**
12:30-13:00	Обеденный перерыв
13:00-19:00	Проведение оценки.
С+1	
время	**план мероприятия**
08:00-22:00	Демонтаж оборудования. Отъезд экспертов

1.4. План застройки площадки для проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия

Компетенция: Сетевое и системное администрирование
Номер компетенции: 39
Дата разработки: «1» октября 2017 г.
План застройки площадки:
Легенда:




2000
1000
1000
25000
1000
4000
4000
4000
6000

2. КОМПЛЕКТ ОЦЕНОЧНОЙ ДОКУМЕНТАЦИИ № 1.1
для демонстрационного экзамена
по стандартам Ворлдскиллс Россия
по компетенции
«Сетевое и системное администрирование»

2.1 Паспорт Комплекта оценочной документации № 1.1

КОД 1. 1 по компетенции «Сетевое и системное администрирование»

разработан в целях организации и проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия по *код и наименование профессии и/или специальности среднего профессионального образования, по которому (ым) проводится демонстрационный экзамен*

(из перечня профессий среднего профессионального образования и перечня специальностей среднего профессионального образования, утвержденных приказом Министерства образования и науки Российской Федерации от 29 октября 2013 года №1199).

1. Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта компетенции «Сетевое и системное администрирование» (WorldSkills Standards Specifications, WSSS), проверяемый в рамках комплекта оценочной документации

	Раздел WSSS
3	**Консультирование и поддержка пользователей** Участник должен знать и понимать: Основные возможности определенного круга ИТ-систем для обеспечения качественной поддержки; Подходы к планированию рабочего процесса с целью обеспечения высокого уровня обслуживания, способного удовлетворить потребности пользователя и организации; Различные методы демонстрации и презентации для поддержки развития навыков и знаний пользователя; Различные методы оценки возможностей пользователя с целью удовлетворения его немедленных потребностей и поощрения к саморазвитию; Различные методики обучения, позволяющие адаптировать процесс обучения с учетом навыков и возможностей пользователей; Тренды и вызовы современной IT-индустрии и способы развития, которые могут быть представлены пользователям; Способы ведения переговоров для различных ситуаций. Участник должен уметь: Заблаговременно поддерживать уровень собственных познаний в сфере информационных технологий; Своевременно (в установленных регламентом рамках) отвечать на запросы как локальных, так и удаленных пользователей; Планировать и постоянно актуализировать планы выполнения

	пользовательских запросов к поддержке для балансировки потребностей пользователей и организации; Точно определять требования пользователя и оправдывать ожидания; Подсчитывать время и стоимость выполнения работы; Выбирать наиболее подходящие способы демонстрации для более точного соответствия подачи материала навыкам и знания аудитории; Эффективно демонстрировать информационные системы пользователям и группам пользователей для предоставления им возможностей к улучшению своих навыков и знаний; Успешно обучать пользователей очно и заочно для успешного разрешения проблем в области ИТ-инфраструктуры, представления новых продуктов, улучшения пользовательских навыков и знаний; Определять возможности к улучшению продукта и общей удовлетворенности пользователя; Формировать точные, своевременные рекомендации в области обновления и приобретения новых IT-продуктов и сервисов для улучшения качества принятия решений; Формировать корректные, отвечающие требованиям и ограничениям, рекомендации на основе запросов и потребностей; Принимать участие в тендерных и закупочных процедурах
4	**Поиск и устранение неисправностей** Участник 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. Участник 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
6	**Настройка, обновление и конфигурация операционных систем** Участник 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. Участник 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** Участник должен знать и понимать: Сетевое окружение; Сетевые протоколы; Процесс построения сети и как сетевые устройства могут быть настроены для эффективного взаимодействия; Типы сетевых устройств. Участник 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. Обобщенная оценочная ведомость

В данном разделе определяются критерии оценки и количество начисляемых баллов (субъективные и объективные)

Общее количество баллов задания/модуля по всем критериям оценки составляет 80.

Раздел	**Критерий**	**Оценки**		
		Судейство	**Объективная**	**Общая**
WSSS Sec.6	Базовая настройка ОС Linux	0	13	13
WSSS Sec.6	Базовая настройка ОС Windows	0	13	13
WSSS Sec. 7	Базовые сетевые технологии	0	13	13
WSSS Sec 3, 4	Базовая настройка ОС Linux Базовая настройка ОС Windows Базовые сетевые технологии	0	6	6
Итого =		0	45	45

3. Количество экспертов, участвующих в оценке выполнения задания

3.1. Минимальное количество экспертов, участвующих в оценке демонстрационного экзамена по стандартам Ворлдскиллс Россия по компетенции «Сетевое и системное администрирование» - 3 чел.

Количество постов-рабочих мест / Количество студентов	1 до 5	6 до 10	11 до 15	16 до 20	21 до 25	26 и более
От 1 до 5	3					
От 6 до 10		3				
От 11 до 15			3			
От 16 до 20				6		
От 21 до 25					9	
От 26 и более						9

3.2. Дополнительное количество экспертов рассчитывается исходя из количества участников демонстрационного экзамена.

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

В соответствии с ИЛ

Инфраструктурный лист для КОД № 1.1 – приложение №2

2.2 Задание для демонстрационного экзамена по стандартам Ворлдскиллс Россия по компетенции «Сетевое и системное администрирование» (образец)

Задание включает в себя следующие разделы:

Формы участия

Модули задания и необходимое время

Критерии оценки

Необходимые приложения

Количество часов на выполнение задания: 6 ч.

1. ФОРМА УЧАСТИЯ

индивидуальная

2. МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ

Модули и время сведены в таблице 1

Таблица 1.

№ п/п	Наименование модуля	Максимальный балл	Время на выполнение
1	Модуль А - Базовая настройка Linux	15	2 часа
2	Модуль В - Базовая настройка Windows	15	2 часа
3	Модуль С – Базовые сетевые технологии	15	2 часа

Модули с описанием работ

Модуль 1: Модуль А - Базовая настройка Linux

Конфигурация хостов

1 Настройте имена хостов в соответствии с диаграммой.
2 Установите следующее ПО на ВСЕ виртуальные машины:
  2.1 Пакет tcpdump
  2.2 Пакет net-tools
  2.3 Редактор vim
  2.4 lynx
  2.5 bind-utils
  2.6 mc
  2.7 nfs-utils
3 На всех хостах сформируйте файл **/etc/hosts** в соответствии с Диаграммой (кроме адреса хоста L-CLI и R-CLI). Данный файл будет применяться во время проверки в случае недоступности DNS-сервисов. Проверка по IP-адресам выполняться не будет.
  3.1 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.
   2.1 В качестве DHCP-сервера используйте L-FW.
      2.1.1 Используйте пул адресов 172.16.100.60 — 172.16.100.75.
      2.1.2 Используете адрес L-SRV в качестве адреса DNS-сервера.
   2.2 В качестве шлюза по умолчанию используйте соответствующий адрес L-FW.
   2.3 Используйте DNS-суффикс **skill39.wsr**
   2.4 DNS-записи типа A и PTR должны обновляться при получении адреса от DHCP-сервера.
3 На L-SRV настройте службу разрешения доменных имен.
   3.1 Сервер должен обслуживать зону **skill39.wsr**
   3.2 Сопоставление имен необходимо организовать в соответствии с Таблицей 1.
   3.3 Запросы, которые выходят за рамки зоны **skill39.wsr** должны пересылаться DNS-серверу ISP. Для проверки используйте доменное имя **worldskills.ru**.
   3.4 Реализуйте поддержку разрешения обратной зоны в соответствии с Таблицей 1.
   3.5 Файлы зон необходимо располагать в **/opt/dns/**
4 На DNS сервере ISP приобретена услуга Secondary DNS для зоны **skill39.wsr**
   4.1 Настройте возможность трансфера зоны **skill39.wsr** в сторону ISP.
   4.2 Используйте адрес ISP в качестве адреса DNS сервера для R-FW и R-CLI.
   4.3 Трансфер зоны на другие хосты, кроме ISP, должен быть запрещен.
5 На L-FW и R-FW настройте интернет-шлюз для организации коллективного доступа в Интернет.
   5.1 Настройте трансляцию сетевых адресов из внутренней сети в адрес внешнего интерфейса соответствующего межсетевого экрана.

Службы централизованного управления и журналирования

1 Разверните LDAP-сервер для организации централизованного управления учетными записями.
  1.1 В качестве сервера выступает L-SRV.
  1.2 Учетные записи создать в соответствии с Таблицей 2.
  1.3 Группы и пользователей создать в соответствии с Таблицей 2.
  1.4 Пользователи должны быть расположены в OU Users.
  1.5 Группы должны быть расположены в OU Groups.
  1.6 Хосты должны аутентифицироваться через LDAP в соответствии с Таблицей 2.
2 На L-SRV организуйте централизованный сбор журналов с хостов.
  2.1 Журналы должны храниться в директории **/opt/logs/**
  2.2 Журналирование должно производиться в соответствии с Таблицей 3.
  2.3 Сообщения в файлах журналов в директории **/opt/logs** не должны дублироваться.

Конфигурация служб удаленного доступа

1 Настройте сервер удаленного доступа на основе технологии OpenVPN:
  1.1 В качестве сервера выступает L-FW.
  1.2 Параметры туннеля
    1.2.1 Устройство TUN
    1.2.2 Протокол UDP
    1.2.3 Применяется сжатие
    1.2.4 Порт сервера 1122
  1.3 Ключевая информация должна быть сгенерирована на R-FW.
  1.4 В качестве адресного пространства подключаемых клиентов использовать сеть 5.5.5.0/27.
  1.5 Хранение всей необходимой (кроме конфигурационных файлов) информации организовать в **/opt/vpn**
2 На OUT-CLI настройте клиент удаленного доступа на основе технологии OpenVPN:
  2.1 Запуск удаленного подключения должен выполняться скриптом **start_vpn.sh**

2.2 Отключение VPN-туннеля должно выполняться скриптом **stop_vpn.sh**
2.3 Скрипты должны располагаться в **/opt/vpn**
2.4 Скрипты должны вызываться из любого каталога без указания пути.

3 Настройте GRE-туннель между L-FW и R-FW:
3.1 Используйте следующую адресацию внутри GRE-туннеля:
3.1.1 L-FW: 10.5.5.1/30
3.1.2 R-FW: 10.5.5.2/30

4 На L-FW настройте удаленный доступ по протоколу SSH:
4.1 Доступ ограничен пользователями **ssh_p** и **ssh_c**
4.1.1 В качестве пароля использовать **ssh_pass**
4.2 SSH-сервер должен работать на порту **1022**.

5 На OUT-CLI настройте клиент удаленного доступа SSH:
5.1 Доступ к серверу L-FW должен происходить автоматически по правильному порту, без его явного указания номера порта в команде подключения.
5.2 Для других серверов по умолчанию должен использоваться порт **22**.
5.3 Доступ к L-FW под учетной записью **ssh_p** должен происходить с помощью аутентификации на основе открытых ключей.

Конфигурация веб служб

1 На R-FW установите и настройте веб-сервер:
1.1 Настройте веб-сайт для внешнего использования **www.skill39.wsr**
1.1.1 Используйте директорию **/var/www/html/out**
1.1.2 Используйте стандартные порты.
1.1.3 Обеспечьте работу сайта по протоколам **http** и **https** (сертификат должен быть сгенерирован на R-FW).
1.1.4 В случае доступности **https** должно происходить автоматическое перенаправление с **http**.
1.1.5 Клиенты должны доверять сертификату сайта.

Конфигурация служб хранения данных

1 Настройте сервер файлового хранилища на основе технологии NFS:
1.1 В качестве сервера должен выступать L-SRV.
1.2 В качестве хранилища используется каталог **/opt/nfs**
1.3 Доступ организуется для чтения и записи.

2 Настройте автоматическое монтирование NFS хранилища для клиентов L-CLI и R-CLI:
   2.1 Используйте **/opt/nfs** в качестве пути для монтирования.
   2.2 Клиенты L-CLI и R-CLI должны монтировать NFS каталог при запуске операционной системы.

Конфигурация параметров безопасности и служб аутентификации

1 Настройте CA на R-FW, используя OpenSSL.
   1.1 Используйте **/etc/ca** в качестве корневой директории CA.
   1.2 Атрибуты CA должны быть следующими:
      1.2.1 Страна RU
      1.2.2 Организация WorldSkills Russia
      1.2.3 CN должен быть установлен как WSR CA
   1.3 Создайте корневой сертификат CA.
   1.4 Все клиентские операционные системы должны доверять CA.
2 Настройте межсетевой экран **iptables** на L-FW и R-FW.
   2.1 Запретите прямое попадание трафика из Интернет во внутренние сети.
   2.2 Разрешите удаленные подключения с использованием OpenVPN на внешний интерфейс маршрутизатора L-FW.
   2.3 Разрешите необходимый трафик для создания GRE туннеля между организациями.
   2.4 Разрешите SSH подключения на соответствующий порт L-FW и R-FW.
   2.5 Для VPN-клиентов должен быть предоставлен полный доступ к локальным сетям организаций LEFT и RIGHT.
   2.6 Разрешите необходимый трафик к серверу L-SRV по транслированным IP-адресам.
   2.7 Организуйте доступность сервиса DNS на L-SRV по внешнему адресу L-FW.
   2.8 Разрешите необходимый трафик для работы веб и файловых служб.
   2.9 Остальные сервисы следует запретить.

Таблица 1 – DNS-имена

Хост	**DNS-имя**
L-CLI	A,PTR: l-cli.skill39.wsr
L-SRV	A,PTR: l-srv.skill39.wsr CNAME: dns.skill39.wsr
L-FW	A: l-fw.skill39.wsr

	CNAME: vpn.skill39.wsr CNAME: ftp.skill39.wsr
R-FW	A: r-fw.skill39.wsr CNAME: www.skill39.wsr
R-CLI	A: r-cli.skill39.wsr

Таблица 2 – Учетные записи LDAP

Группа	CN	Пароль	Доступ
Administrators	tux	toor	L-CLI L-FW
Users	user1 – user99	P@ssw0rd	L-CLI

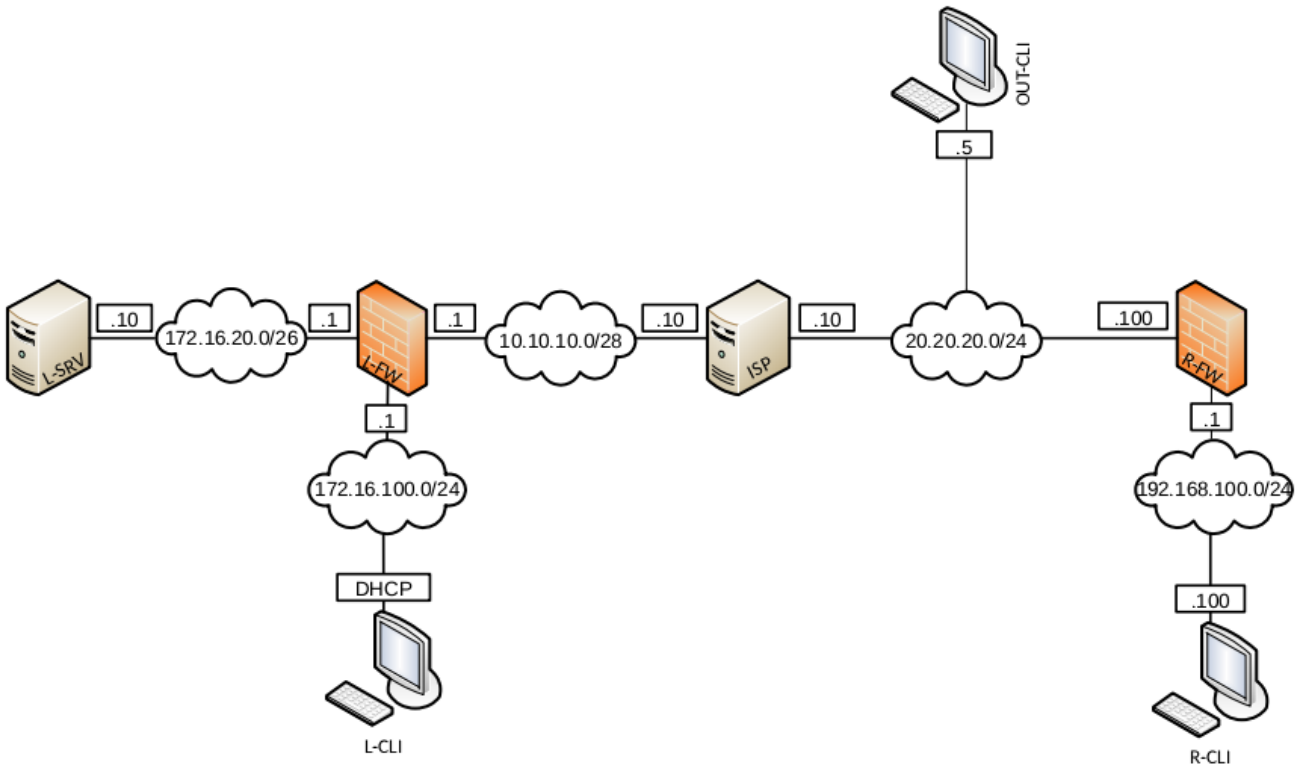
Таблица 3 – Правила журналирования

Источник	Уровень журнала	Файл
L-SRV L-FW	critical	/opt/logs/<HOSTNAME>/crit.log
L-SRV	auth.*	/opt/logs/<HOSTNAME>/auth.log
L-FW	*.err	/opt/logs/<HOSTNAME>/error.log
L-CLI R-CLI	*.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 2: Модуль B - Базовая настройка Windows

Настройка DC1

Базовая настройка

- переименуйте компьютер в DC1;
- перед установкой сетевых настроек решите задачу: вам дано адресное пространство следующего вида – «10.10.18.x/?». Длину маски рассчитайте исходя из того, чтобы в каждой образовавшейся подсети можно было разместить ровно 14 клиентов. Для адресации в домене Pest.com используйте третью по счету подсеть; в качестве адреса DC1 используйте первый возможный адрес из этой подсети;
- обеспечьте работоспособность протокола ICMP (для использования команды ping).

Active Directory

- сделайте сервер контроллером домена Pest.com.

DHCP

- настройте протокол DHCP для автоконфигурации клиентов – в качестве диапазона выдаваемых адресов используйте все не занятые серверами адреса в подсети;
- настройте failover: mode – Load balancer, partner server – SRV1, state switchover – 10 min;
- настройте дополнительные свойства области (адреса DNS-серверов и основного шлюза).

DNS

- настройте необходимые зоны прямого и обратного просмотра;
- создайте вручную все необходимые записи типа A и PTR для серверов домена и необходимых web-сервисов.

GPO

- запретите анимацию при первом входе пользователей в систему на всех клиентских компьютерах домена;
- в браузерах IE Explorer и Microsoft Edge (установите и используйте windows10.admx) должна быть настроена стартовая страница – www.Pest.com;

Элементы доменной инфраструктуры

- создайте подразделения: Experts, Competitors, Managers, Visitors и IT;
- в соответствующих подразделениях создайте доменные группы: Experts, Competitors, Managers, Visitors, IT;

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.

- 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;
- для каждого пользователя создайте автоматически подключаемую в качестве диска U:\ домашнюю папку по адресу SRV1→d:\shares\users;

Настройка SRV1

Базовая настройка

- переименуйте компьютер в SRV1;
- перед установкой сетевых настроек решите задачу: вам дано адресное пространство следующего вида – «10.10.18.x/?». Длину маски рассчитайте исходя из того, чтобы в каждой образовавшейся подсети можно было разместить ровно 14 клиентов. Для адресации в домене Pest.com используйте третью по счету подсеть; в качестве адреса SRV1 используйте второй возможный адрес из этой подсети;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к домену Pest.com;
- с помощью дополнительных жестких дисков создайте зеркальный массив; назначьте ему букву D:\.

Active Directory

- сделайте сервер дополнительным контроллером домена Pest.com.

DHCP

- настройте протокол DHCP для автоконфигурации клиентов;
- настройте failover: mode – Load balancer, partner server – DC1, state switchover – 10 min;

DNS

- сделайте сервер дополнительным DNS-сервером в домене Pest.com;
- загрузите с DC1 все зоны прямого и обратного просмотра.

Общие папки

- создайте общие папки для подразделений (Competitors, Experts and Managers) по адресу SRV1→d:\shares\departments;
- обеспечьте привязку общей папки подразделения к соответствующей группе в качестве диска G:\.

Квоты/Файловые экраны

- установите максимальный размер в 1Gb для каждой домашней папки пользователя (U:\);
- запретите хранение в домашних папках пользователей файлов с расширениями .mp3 и .wav; учтите, что файлы остальных типов пользователи вправе хранить в домашних папках.

IIS

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

Настройка DCA

Базовая настройка

- переименуйте компьютер в DCA;
- перед установкой сетевых настроек решите задачу: вам дано адресное пространство следующего вида – «10.10.18.x/?». Длину маски рассчитайте исходя из того, чтобы в каждой образовавшейся подсети можно было разместить ровно 14 клиентов. Для адресации в домене Pest.com используйте третью по счету подсеть; в качестве адреса DCA используйте третий возможный адрес из этой подсети;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к домену Pest.com.

Службы сертификации

- установите службы сертификации;
- настройте основной доменный центр сертификации;

- имя центра сертификации – Pest CA;
- срок действия сертификата – 10 лет;
- настройте шаблон выдаваемого сертификата для клиентских компьютеров *ClientComps*: *subject name=common name*, автозапрос для компьютера BRIDGE1;
- настройте шаблон выдаваемого сертификата для группы Managers *ManUsers*: *subject name=common name*, автозапрос только для пользователей – членов группы Managers.

Настройка CLI1

Базовая настройка

- переименуйте компьютер в CLI1;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к домену Pest.com;
- установите набор компонентов удаленного администрирования RSAT;
- запретите использование «спящего режима» таким образом, чтобы пользователи домена не могли изменить эту настройку без участия администратора домена;
- используйте компьютер для тестирования настроек в домене Pest.com: пользователей, общих папок, групповых политик, в том числе – тестирования удаленных подключений через Direct Access (временно переключая компьютер в сеть Internet).

Настройка DC2

Базовая настройка

- переименуйте компьютер в DC2;
- перед установкой сетевых настроек решите задачу: вам дано адресное пространство следующего вида – «192.168.19.y/?». Длину маски рассчитайте исходя из того, чтобы в данном пространстве имелось ровно 8 подсетей. Для адресации в поддомене Buda.Pest.com используйте вторую по счету подсеть; в качестве адреса DC2 используйте первый возможный адрес из этой подсети;
- обеспечьте работоспособность протокола ICMP (для использования команды ping).

Active Directory

- сделайте сервер контроллером поддомена Buda.Pest.com.

DHCP

- настройте протокол DHCP для автоконфигурации клиентов – в качестве диапазона выдаваемых адресов используйте все не занятые серверами адреса в подсети.

DNS

- настройте необходимые зоны прямого и обратного просмотра;
- создайте вручную все необходимые записи типа A и PTR для серверов домена и необходимых web-сервисов;
- обеспечьте разрешение имен сайтов www.pest.com и www.buda.pest.com (оба сайта должны быть доступны со всех клиентских компьютеров сети предприятия).

GPO

- настройте необходимые политики, обеспечивающие использование сервера DCA.Pest.com в качестве доверенного центра сертификации.

Настройка SRV2

Базовая настройка

- переименуйте компьютер в SRV2;
- перед установкой сетевых настроек решите задачу: вам дано адресное пространство следующего вида – «192.168.19.y/?». Длину маски рассчитайте исходя из того, чтобы в данном пространстве имелось ровно 8 подсетей. Для адресации в поддомене Buda.Pest.com
- используйте вторую по счету подсеть; в качестве адреса SRV2 используйте второй возможный адрес из этой подсети;
- обеспечьте работоспособность протокола ICMP (для использования команды ping).

IIS

- создайте сайт www.pest.com (используйте предоставленный htm-файл в качестве документа по умолчанию);
- создайте сайт www.buda.pest.com (используйте предоставленный htm-файл в качестве документа по умолчанию);
- оба сайта должны быть доступны по протоколу https с использованием сертификатов, выданных DCA.

Настройка CLI2

Базовая настройка

- переименуйте компьютер в CLI2;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к поддомену Buda.Pest.com;
- запретите использование «спящего режима» таким образом, чтобы пользователи поддомена не могли изменить эту настройку без участия администратора поддомена;
- используйте компьютер для тестирования настроек в поддомене Buda.Pest.com.

Настройка BRIDGE2

Базовая настройка

- переименуйте компьютер в BRIDGE2;
- задайте настройки сети следующим образом: для сетевого интерфейса, подключенного к inet используйте адрес 200.100.100.1/24; для сетевого адреса в подсети buda.pest.com используйте последний возможный адрес из рассчитанной ранее подсети;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к поддомену Buda.Pest.com.

Настройка RRAS

- установите службу RRAS;
- настройте VPN-соединение с доменом Pest.com по протоколу PPTP; весь трафик между доменами должен передаваться через это соединение.

Настройка BRIDGE1

Базовая настройка

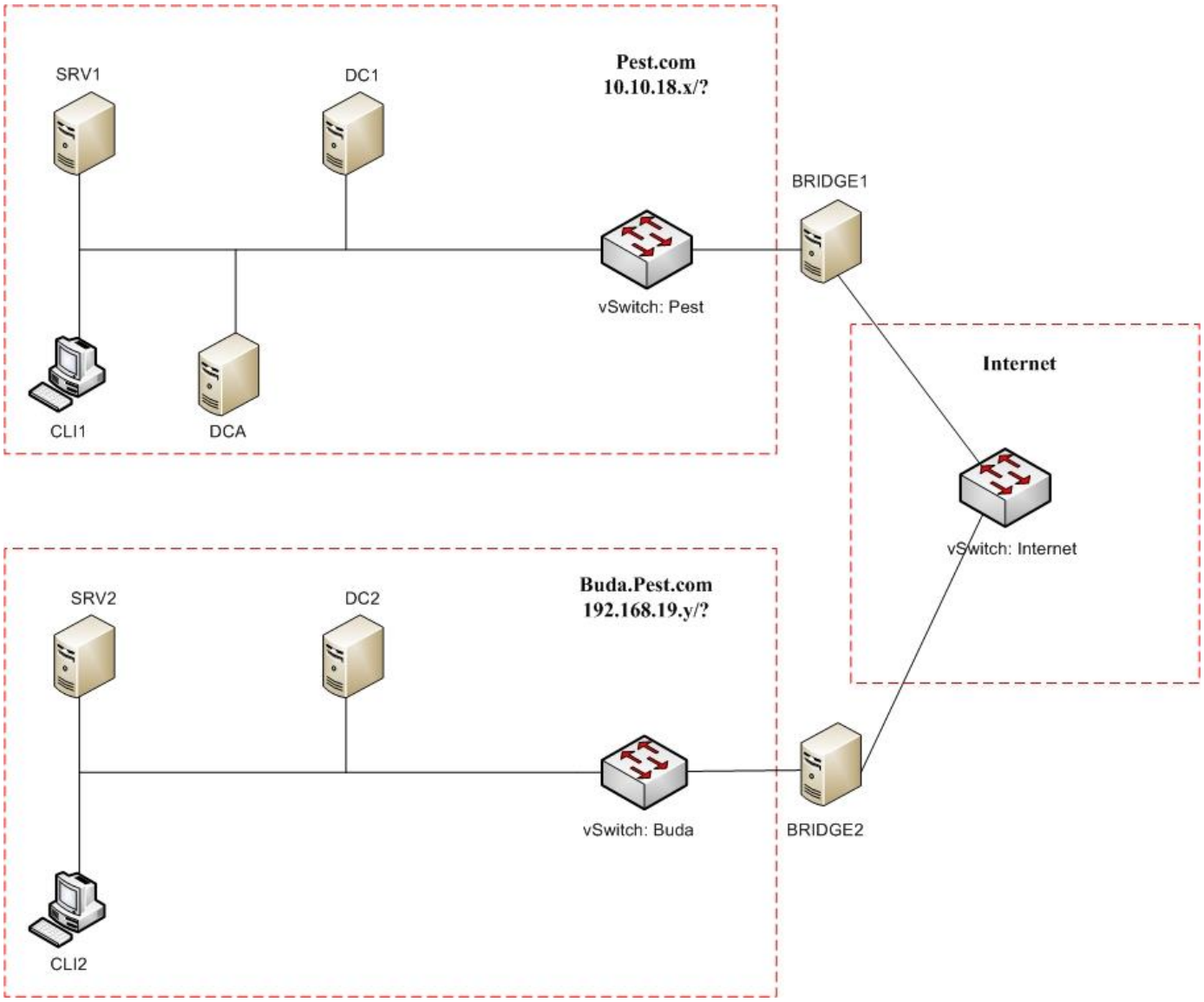
- переименуйте компьютер в BRIDGE1;
- задайте настройки сети следующим образом: для сетевого интерфейса, подключенного к inet используйте адрес 200.100.50.1/24; для сетевого адреса в подсети pest.com используйте последний возможный адрес из рассчитанной ранее подсети;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к домену Pest.com.

Настройка RRAS

- установите службу RRAS;

– настройте защищенное VPN-соединение с поддоменом buda.pest.com по протоколу PPTP; весь трафик между доменами должен передаваться через это соединение.

ДИАГРАММА ВИРТУАЛЬНОЙ СЕТИ



Модуль 3: Модуль C – Базовые сетевые технологии

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**
   3.1 Пароль пользователя должен храниться в конфигурации в виде результата хэш-функции.
   3.2 Пользователь должен обладать максимальным уровнем привилегий.
4 На всех устройствах установите пароль **wsr** на вход в привилегированный режим.
   4.1 Пароль должен храниться в конфигурации НЕ в виде результата хэш-функции.
   4.2 Настройте режим, при котором все пароли в конфигурации хранятся в зашифрованном виде.
5 Для всех устройств реализуйте модель AAA.
   5.1 Аутентификация на линиях виртуальных терминалов с 0 по 15 должна производиться с использованием локальной базы учётных записей. (кроме маршрутизатора HQ1)
   5.2 После успешной аутентификации при удалённом подключении пользователи сразу должен получать права, соответствующие их уровню привилегий или роли (кроме межсетевого экрана FW1).
   5.3 Настройте необходимость аутентификации на локальной консоли.
   5.4 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, подинтерфейсы 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.
   7.1 Используйте на линиях vty с 0 по 4 отдельный список методов с названием method_man
   7.2 Порядок аутентификации:
      7.2.1 По протоколу RADIUS
      7.2.2 Локальная
   7.3 Используйте общий ключ **cisco**

7.4 Используйте номера портов 1812 и 1813 для аутентификации и учета соответственно

7.5 Адрес RADIUS-сервера 172.16.20.2

7.6 Настройте авторизацию при успешной аутентификации

7.7 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**.

1.1 В качестве основного сервера VTP настройте SW1.

1.2 Коммутаторы SW2 и SW3 настройте в качестве VTP клиента.

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

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

1.5 Таблица VLAN должна содержать следующие сети:

1.5.1 VLAN100 с именем MGT.

1.5.2 VLAN200 с именем DATA.

1.5.3 VLAN300 с именем OFFICE.

1.5.4 VLAN 400

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

2.1 Порты F0/10 коммутаторов SW1 и SW3, а также порт F0/24 коммутатора SW2 должны быть работать в режиме доступа без использования согласования. Отключите протокол DTP явным образом.

2.2 Транк между коммутаторами SW2 и SW3 должен быть настроен без использования согласования. Отключите протокол DTP явным образом.

2.3 Транки между коммутаторами SW1 и SW2, а также между SW1 и SW3, должны быть согласованы по DTP, коммутатор SW1 должен инициировать создание транка, а коммутаторы SW2 и SW3 должны ожидать начала согласования параметров от соседа, но сами не инициировать согласование.

3 Настройте агрегирование каналов связи между коммутаторами.

3.1 Номера портовых групп:

1 – между коммутаторами SW1 (F0/1-3) и SW2 (F0/1-3);

2– между коммутаторами SW2 (F0/6-7) и SW3 (F0/6-7);

3.2 Агрегированный канал между SW1 и SW2 должен быть организован с использованием протокола согласования LACP. SW1 должен быть настроен в активном режиме, SW2 в пассивном.

3.3 Агрегированный канал между SW2 и SW3 должен быть организован с использованием протокола согласования PAgP. SW2 должен быть настроен в предпочтительном, SW3 в автоматическом.

4 Конфигурация протокола остовного дерева:

4.1 Используйте протокол Rapid STP.

4.2 Коммутатор SW1 должен являться корнем связующего дерева в сетях VLAN 100, 200 и 300, в случае отказа SW1, корнем должен стать коммутатор SW2.

4.3 Настройте используемые порты коммутаторов SW1 и SW2 так, чтобы во всех VLAN корнем связующего дерева могли стать только SW1 или SW2, а при получении BPDU пакета с лучшим приоритетом корня, порт должен перейти в состояние root-inconsistent.

4.4 Настройте порт F0/10 коммутатора SW2, 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 коммутаторов SW1, SW2 и порт F0/24 коммутатора SW3, в соответствии с L2 диаграммой. Порты должны быть настроены в режиме доступа.

6 Отключите протокол CDP на маршрутизаторах HQ1 и BR1, только на портах в сторону провайдера ISP1.

Настройка подключений к глобальным сетям

1 Настройте подключение PPPoE между ISP1 и маршрутизатором BR1.

1.1 Настройте PPPoE клиент на BR1.

1.2 Используйте имя пользователя **cisco** и пароль **cisco**

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

1.4 BR1 должен автоматически получать адрес от ISP1.

2 Настройте подключение HQ1 к провайдеру ISP1 с помощью протокола PPP.

2.1 Настройте Multilink PPP с использованием двух Serial-интерфейсов.

2.2 Используйте 1 номер интерфейса.

2.3 Не используйте аутентификацию.

2.4 HQ1 должен автоматически получать адрес от ISP2.

3 FW1 подключена к провайдеру ISP1 с помощью IPoE и имеет статический адрес.

Настройка маршрутизации

1 В офисе HQ, на устройствах HQ1 и FW1 настройте протокол динамической маршрутизации OSPF.
   1.1 Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
   1.2 Используйте область с номером 51 для всех сетей центрального офиса.
   1.3 HQ1 и FW1 должны устанавливать соседство только в сети 172.16.0.12/30.
   1.4 Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.
2 Настройте протокол динамической маршрутизации OSPF в офисе BR1 с главным офисом HQ.
   2.1 Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
   2.2 Используйте магистральную область для GRE туннеля.
   2.3 Соседства между офисами HQ и BR1 должны устанавливаться через защищенный туннель.
   2.4 В офисе BR1 используйте область с номером 1.
   2.5 Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.
3 ISP1 предоставляет подсеть PA (Provider Aggregatable) адресов (11.11.11.11/32) для офиса BR1. На маршрутизаторе BR1 настройте протокол динамической маршрутизации EIGRP с номером автономной системы **2018**.
   3.1 Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
   3.2 Используйте аутентификацию MD5 с помощью связки ключей EIGRP с ключом **WSR** и номером ключа **2**.
   3.3 Провайдер ISP1 выполняет редистрибуцию маршрута 11.11.11.11/32 в сеть BGP, убедитесь в том, что вы корректно анонсируете данный маршрут провайдеру.
4 Офис HQ имеет подсети PI (Provider Independent) адресов и автономную систему 65000. На маршрутизаторе и межсетевом экране настройте протокол динамической маршрутизации BGP в соответствии с таблицей

Устройство	AS
HQ1	65000
FW1	65000
ISP1	65001

4.1 Настройте автономные системы в соответствии с Routing-диаграммой.
4.2 Маршрутизатор HQ1 и FW1 должны быть связаны с помощью iBGP. Используйте для этого соседства, интерфейсы, которые находятся в подсети 172.16.0.12/30.
4.3 Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.

5 Настройте прокол динамической маршрутизации OSPFv3 поверх защищенного туннеля. На маршрутизаторах HQ1 и BR1 настройте протокол динамической маршрутизации OSPFv3 с номером процесса 1.
5.1 Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
5.2 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.
1.1 Передача данных между HQ1 и SRV1 осуществляется без аутентификации.
1.2 Настройте временную зону с названием MSK, укажите разницу с **UTC +3** часов.
1.3 Настройте сервер синхронизации времени. Используйте стратум **2**.
1.4 Используйте для синхронизации клиентов с HQ1 аутентификацию MD5 с ключом **WSR**.

2 Настройте динамическую трансляцию портов (PAT):
2.1 На маршрутизаторе BR1 настройте динамическую трансляцию портов (PAT) для сети 192.168.1.0/24 в адрес петлевого интерфейса 11.11.11.11.

3 Настройте протокол динамической конфигурации хостов со следующими характеристиками
3.1 На маршрутизаторе HQ1 для подсети OFFICE:
3.2 Адрес сети – 30.30.30.0/24.

3.3 Адрес шлюза по умолчанию интерфейс роутера HQ1.
3.4 Адрес TFTP-сервера 172.16.20.2.
3.5 Компьютер PC1 должен получать адрес 30.30.30.30.

Настройка механизмов безопасности

1 На маршрутизаторе BR1 настройте пользователей с ограниченными правами.
1.1 Создайте пользователя **user1** с паролем **cisco**
1.2 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.
2 На коммутаторе SW3 включите DHCP Snooping для подсети OFFICE. Используйте флеш-память в качестве места хранения базы данных.
3 На коммутаторе SW3 включите динамическую проверку ARP-запросов в сети OFFICE. Сделайте порт Fa0/11 доверенным.

Настройка параметров мониторинга и резервного копирования

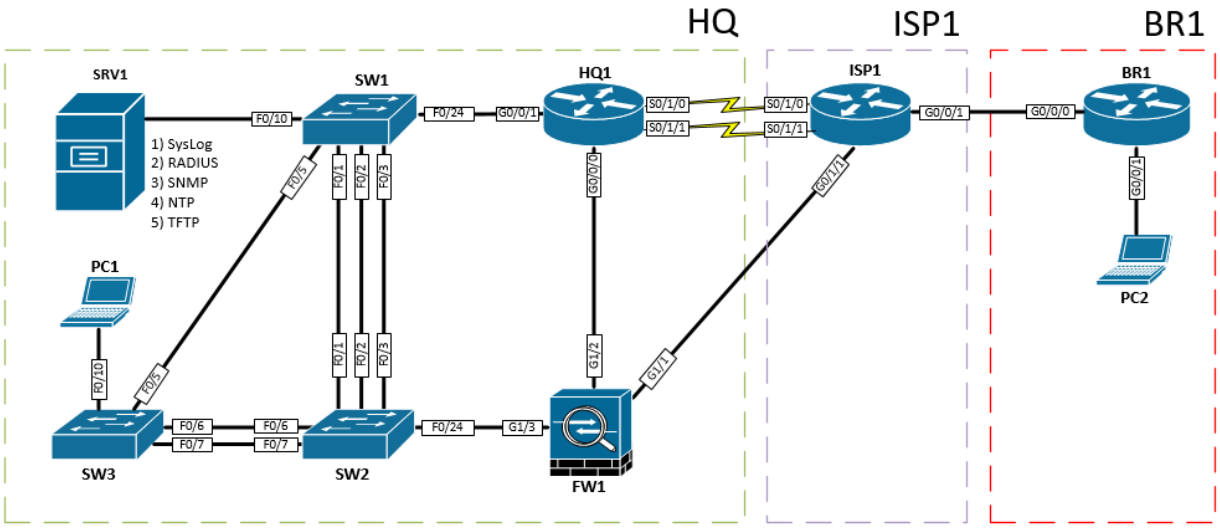
1 На маршрутизаторе HQ1 и межсетевом экране FW1 настройте возможность удаленного мониторинга по протоколу SNMP v3.
1.1 Задайте местоположение устройств EKB, Russia
1.2 Задайте контакт admin@wsr.ru
1.3 Используйте имя группы WSR.
1.4 Создайте профиль только для чтения с именем RO.
1.5 Используйте для защиты SNMP шифрование AES128 и аутентификацию SHA1.
1.6 Используйте имя пользователя: **snmpuser** и пароль: **snmppass**
1.7 Для проверки вы можете использовать команду snmp_test_HQ и snmp_test_FW на SRV1.

Конфигурация виртуальных частных сетей

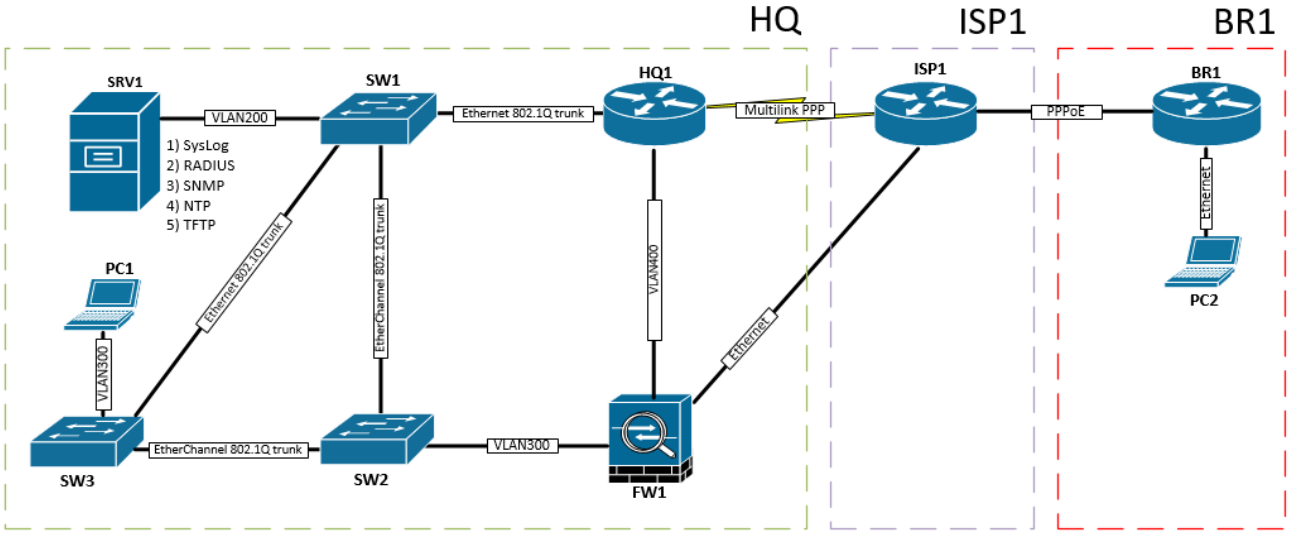
1 На маршрутизаторах HQ1 и BR1 настройте DMVPN:
1.1 Используйте в качестве VTI интерфейс Tunnel1
1.2 Используйте адресацию в соответствии с L3-диаграммой
1.3 Режим — GRE multipoint
1.4 Интерфейс-источник — Loopback-интерфейс на каждом маршрутизаторе.
1.5 Идентификатор сети – 100.

Аутентификация по ключу cysco

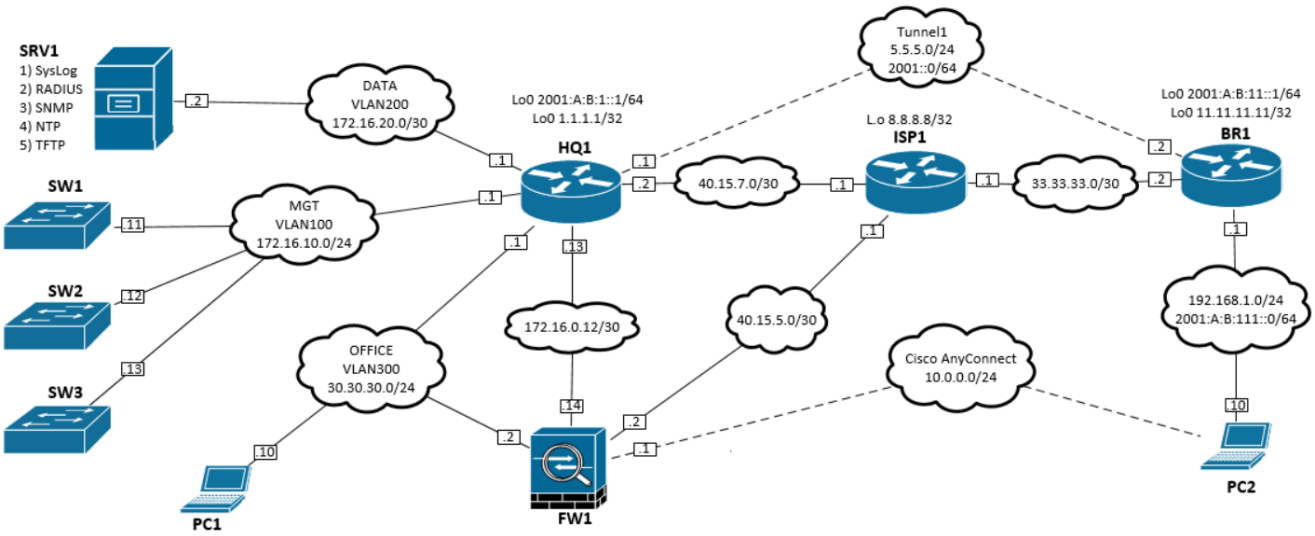
Топология L1



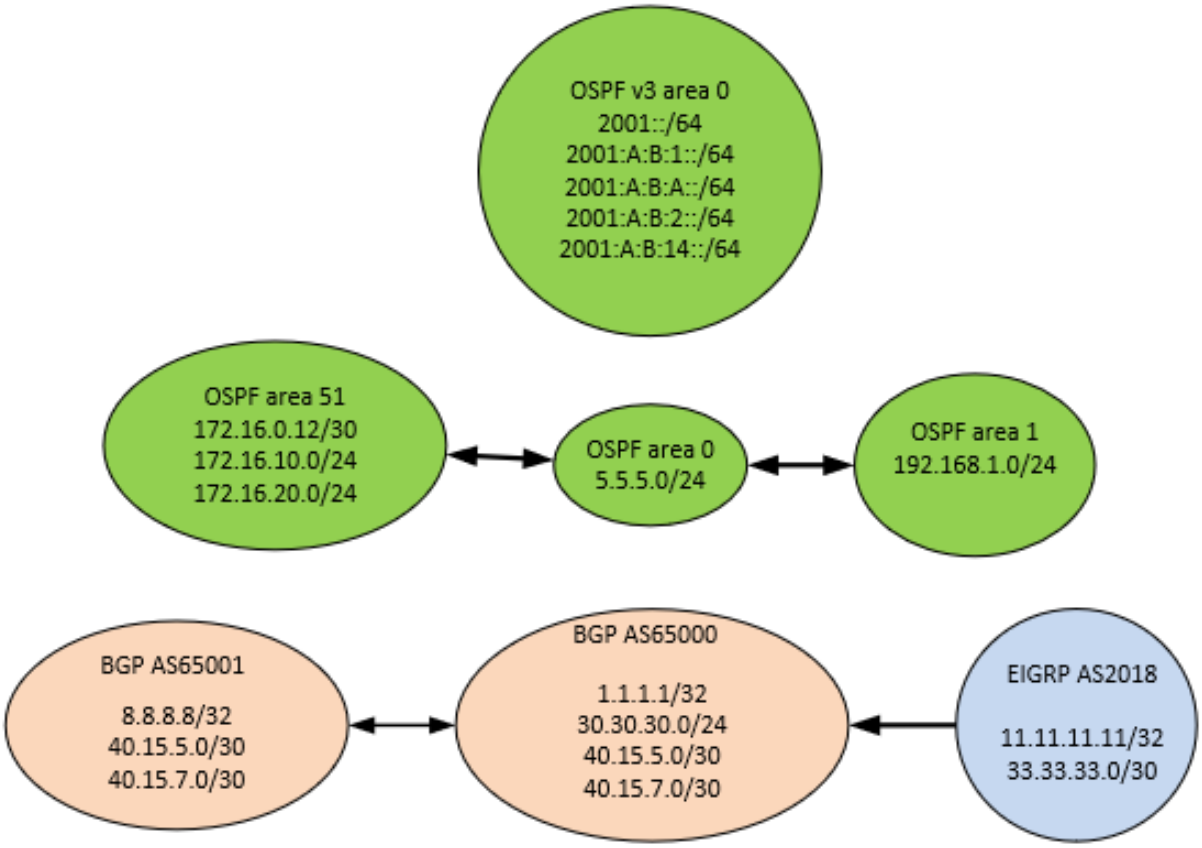
Топология L2



Топология L3


SRV1
1) SysLog
2) RADIUS
3) SNMP
4) NTP
5) TFTP
.2
DATA
VLAN200
172.16.20.0/30
.1
Lo0 2001:A:B:1::1/64
Lo0 1.1.1.1/32
HQ1
Tunnel1
5.5.5.0/24
2001::0/64
.1
.2
40.15.7.0/30
.1
L.o 8.8.8.8/32
ISP1
.1
33.33.33.0/30
.2
Lo0 2001:A:B:11::1/64
Lo0 11.11.11.11/32
BR1
.2
.1
SW1
.11
MGT
VLAN100
172.16.10.0/24
.1
SW2
.12
SW3
.13
.1
.13
172.16.0.12/30
40.15.5.0/30
.1
192.168.1.0/24
2001:A:B:111::0/64
.1
OFFICE
VLAN300
30.30.30.0/24
.14
.2
.1
Cisco AnyConnect
10.0.0.0/24
.10
.10
PC1
FW1
PC2

Routing-диаграмма



3. КРИТЕРИИ ОЦЕНКИ

В данном разделе определены критерии оценки и количество начисляемых баллов (субъективные и объективные) в Таблице 2.

Общее количество баллов задания/модуля по всем критериям оценки составляет ___.

Таблица 2.

Раздел	**Критерий**	**Оценки**		
		Судейство	**Объективная**	**Общая**
WSSS Sec.6	Базовая настройка ОС Linux	0	13	13
WSSS Sec.6	Базовая настройка ОС Windows	0	13	13
WSSS Sec. 7	Базовые сетевые технологии	0	13	13
WSSS Sec 3, 4	Базовая настройка ОС Linux Базовая настройка ОС Windows Базовые сетевые технологии	0	6	6
Итого =		0	45	45

Субъективные оценки -0.

4. НЕОБХОДИМЫЕ ПРИЛОЖЕНИЯ

Нет.

2.3 План проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия

Данное задание рассчитано на 1 день или 8 часов. План экзамена будет структурирован следующим образом:

За два дня до экзамена должно быть полностью готово оборудование. В этот же день необходимо провести собрание экспертов, на котором пройти необходимый инструктаж. Эксперты должны чётко понимать свои роли и функции, а также планируемый график работы.

За день до экзамена необходимо зарегистрировать участников, проверить паспорта и провести для них необходимый инструктаж. После прохождения инструктажа по технике безопасности и охране труда участники могут приступить к ознакомлению с рабочими местами. Рекомендуется выделить не менее 30 минут на каждый из модулей. По завершению ознакомления технический эксперт должен вернуть рабочие места к исходному состоянию и убедиться, что всё готово к началу экзамена.

В днь проведения экзамена проводится краткий брифинг и жеребьёвка по рабочим местам. В первый день при жеребьёвке определяется порядок выполнения модулей (Linux – Windows – Cisco, Windows – Cisco – Linux, Cisco – Linux – Windows) и номер рабочего места в этот день. После этого участники приступают к выполнению одного из модулей A, B и C – согласно жеребьёвке. На модуль отводится 2 часа. Завершая выполнение этого модуля, участники уходят на обед. После обеда участники приступают к выполнению следующего модуля.

Проверка выполнения задания начинается после завершения выполнения всех модулей. Начать проверку раньше не следует. Проверка организуется параллельно с выполнением в отдельном помещении.

План проведения демонстрационного экзамена корректируется главным экспертом площадки проведения демонстрационного экзамена в зависимости от времени, выделенного на площадке проведения демонстрационного экзамена, количества участников и рабочих мест.

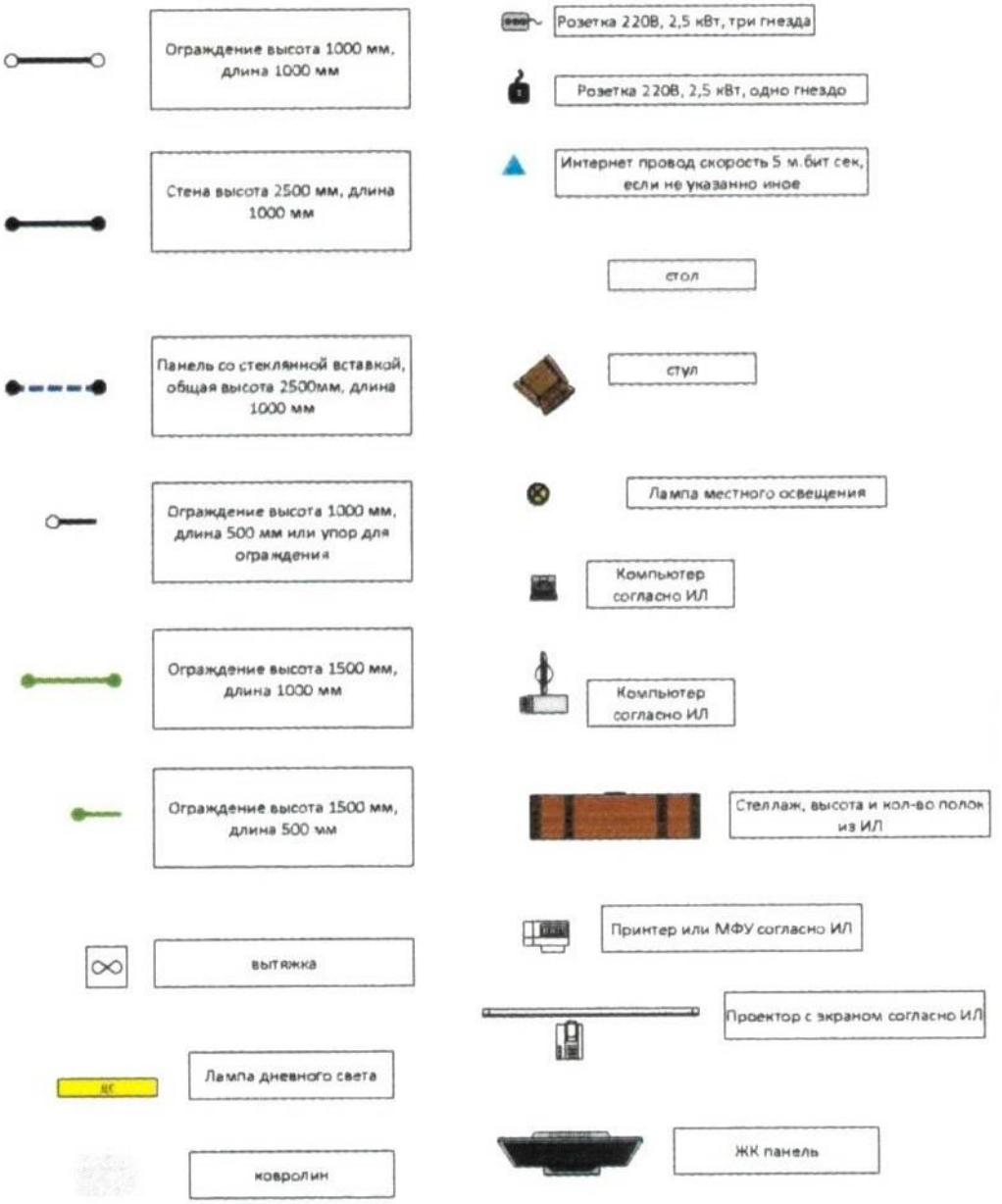
Пример плана проведения:

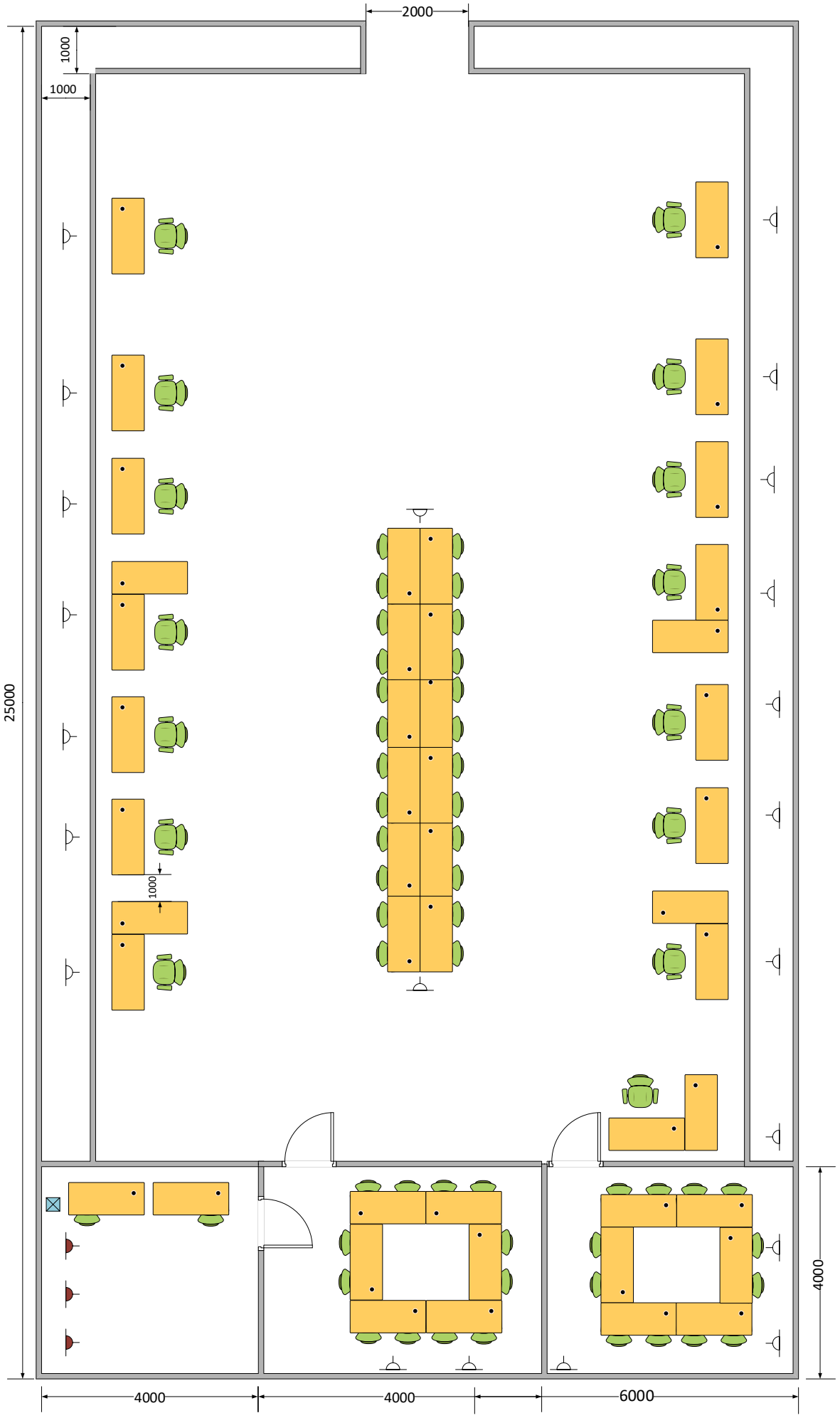
день	С-2	С-1	С1	С+1
дата				
описание	Подготовительные дни		Дни экзамена	Отъезд

С-2	
время	**план мероприятия**
09:00-18:00	Завершение застройки и монтажа мебели, оргтехники, стендов и оборудования
09:00-18:00	Приезд экспертов
18:00-19:00	Собрание экспертов. Инструктаж. Распределение ролей и формирование групп оценки.
С-1	
время	**план мероприятия**
13:00-13:30	Регистрация участников на конкурсной площадке
13:30-14:00	Инструктаж участников по ОТ и ТБ
14:00-16:00	Ознакомление с рабочими местами и оборудованием.
16:00-18:00	Подготовка конкурсных мест. Проверка оборудования.
С1	
время	**план мероприятия**
08:00-08:30	Сбор участников и экспертов на площадке
08:30-09:00	Брифинг для участников, жеребьевка
09:00-11:00	**Выполнение задания (Модули A/B/C)**
11:00-12:30	Обеденный перерыв
12:30-14:30	**Выполнение задания (Модули A/B/C)**
14:30-15:00	Чайная пауза
15:00-17:00	**Выполнение задания (Модули A/B/C)**
17:00-21:00	Проведение оценки.
С+1	
время	**план мероприятия**
08:00-22:00	Демонтаж оборудования. Отъезд экспертов

2.4 План застройки площадки для проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия

Компетенция: Сетевое и системное администрирование
Номер компетенции: 39
Дата разработки: «1» октября 2017 г.
План застройки площадки:
Легенда:




2000
1000
1000
25000
1000
4000
4000
4000
6000

ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Организация, принявшая решение о проведении демонстрационного экзамена (далее – организация), из комплектов оценочной документации, содержащихся в настоящих Оценочных материалах, выбирает один КОД, о чем уведомляет Союз не позднее, чем за три месяца до даты проведения.

Выбирая КОД в качестве материалов для организации подготовки к демонстрационному экзамену, организация соглашается с:

а) уровнем и сложностью задания для демонстрационного экзамена, включая максимально возможный балл;

б) требованиями к оборудованию, оснащению и расходным материалам для проведения демонстрационного экзамена;

в) перечнем знаний, умений и навыков, подлежащих оценке в рамках демонстрационного экзамена;

г) требованиями к составу экспертных групп для оценки выполнения заданий.

В соответствии с выбранным КОД образовательная организация, проводящая демонстрационный экзамен в рамках промежуточной или государственной итоговой аттестации, корректирует образовательные программы по соответствующим профессиям, специальностям и направлениям подготовки, разрабатывает регламентирующие документы и организует подготовку к демонстрационному экзамену. При этом, выбранный КОД утверждается образовательной организацией в качестве требований к проведению выпускной квалификационной работы в виде демонстрационного экзамена без внесения в него каких-либо изменений.

Не допускается внесение изменений в утвержденные КОД, исключение элементов или их дополнение, включая оценочную схему.

При выявлении на площадках проведения демонстрационного экзамена любых случаев внесения изменений в утвержденные КОД, Союз оставляет за собой право аннулировать результаты демонстрационного экзамена с последующим лишением статуса центра проведения демонстрационного экзамена и применением мер взыскания в отношении членов экспертной группы в рамках своих полномочий.

ПРИЛОЖЕНИЯ

Приложение №1 – Инфраструктурный лист для КОД № 2.1
Приложение №2 – Инфраструктурный лист для КОД № 1.1