Конкурсное задание

КОМПЕТЕНЦИЯ «СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

Конкурсное задание включает в себя следующие разделы:

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

Количество часов на выполнение задания: 15 ч.

1) ФОРМЫ УЧАСТИЯ В КОНКУРСЕ

Индивидуальный конкурс.

2) ЗАДАНИЕ ДЛЯ КОНКУРСА

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

Задание национального финала является утвержденным. В нем присутствуют 3 из 5 модулей, т.е. возможно набрать максимально 45 из 100 баллов

Конкурс включает в себя “Пусконаладку инфраструктуры на основе ОС семейства Linux”; “Пусконаладку инфраструктуры на основе ОС семейства Windows”; “Пусконаладку телекоммуникационного оборудования”.

Окончательная методика проверки уточняются членами жюри. Оценка производится в отношении работы модулей. Если участник конкурса не выполняет требования техники безопасности, подвергает опасности себя или других конкурсантов, такой участник может быть отстранен от конкурса.

Время и детали конкурсного задания в зависимости от конкурсных условий могут быть изменены членами жюри, по согласованию с менеджером компетенции.

Конкурсное задание должно выполняться в формате “один модуль в день”, циклически по модулям A-B-C. Оценка каждого модуля происходит ежедневно.

Собранные OVA-образа для модуля Linux и Windows доступны по ссылке:
https://shorturl.at/bntwA

Оперативную помощь по развертыванию стендов можно получить в телеграмм чате компетенции:
https://shorturl.at/vyRX9

Задания разработаны и протестированы группой сертифицированных экспертов:

Таблица 1 – Группа сертифицированных экспертов

Модуль конкурсного задания	Роль	ФИО Эксперта
Модуль A: «Пусконаладка инфраструктуры на основе ОС семейства Linux»	Ведущий разработчик	М.М. Фучко
	Группа разработки	А.Г. Уймин, Д.С. Лавров
Модуль B: «Пусконаладка инфраструктуры на основе ОС семейства Windows»	Ведущий разработчик	М.А. Афанасьев
	Группа разработки	Д.В. Дюгуров
Модуль C: «Пусконаладка телекоммуникационного оборудования»	Ведущий разработчик	Д.С. Лавров
	Группа разработки	Д.А. Букин, А.Г. Уймин

3. МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ

Модули и время приведены в таблице 2.

Таблица 2 – Время выполнение модуля

№ п/п	Наименование модуля	Рабочее время	Время на задание
1	Модуль А: «Пусконаладка инфраструктуры на основе ОС семейства Linux»	В соответствии с жеребьевкой по циклу А-В-С	5 ч.
2	Модуль В: «Пусконаладка инфраструктуры на основе ОС семейства Windows»		5 ч.
3	Модуль С: «Пусконаладка телекоммуникационного оборудования»		5 ч.

ВВЕДЕНИЕ

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

ОПИСАНИЕ КОНКУРСНОГО ЗАДАНИЯ

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

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

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

ИНСТРУКЦИИ ДЛЯ УЧАСТНИКА

В первую очередь необходимо прочитать задание полностью. Следует обратить внимание, что задание составлено не в хронологическом порядке. Некоторые секции могут потребовать действий из других секций, которые изложены ниже. На вас возлагается ответственность за распределение своего рабочего времени. Не тратьте время, если у вас возникли проблемы с некоторыми заданиями. Вы можете использовать временные решения (если у вас есть зависимости в технологическом стеке) и продолжить выполнение других задач. Рекомендуется тщательно проверять результаты своей работы.

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

Если Вам требуется установить пароль, (и он не указан в задании) используйте: “P@ssw0rd”.

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

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

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

НЕОБХОДИМОЕ ОБОРУДОВАНИЕ, ПРИБОРЫ, ПО И МАТЕРИАЛЫ

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

В качестве системной ОС в организации **LEFT** используется **CentOS 8**

В качестве системной ОС в организации **RIGHT** используется **CentOS 8**

В обоих офисах возможно замещение ОС на Alt Linux

Для установки дополнительных пакетов, вам доступны интернет репозитории через YUM-Proxy **http://10.10.10.10:3128**

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

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

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

СХЕМА ОЦЕНКИ

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

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

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

Базовая настройка

1) Настройте имена хостов в соответствии с **Диаграммой.**
2) Если необходимо, сформируйте файл /etc/hosts. Данный файл будет использован при проверке, в случае неработоспособности DNS.
3) В случае корректной работы DNS-сервисов ответы DNS должны иметь более высокий приоритет.
4) Разработайте адресацию для сетей на ваше усмотрение.
5) ***Все хосты должны быть доступны аккаунту root по SSH на стандартном(22) порту***

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 172.16.100.65 — 172.16.100.75 для сети L-RTR-A
        ii) Используйте пул адресов 172.16.200.65 — 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 и PTR 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 и R-FW настройте интернет-шлюзы 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. www.skill39.wsr должен преобразовываться во внешний адрес R-FW.

Конфигурация систем централизованного управления пользователями и компьютерами

1) Разверните LDAP-сервер для организации централизованного управления учетными записями на базе 389 Directory Server
    a) В качестве сервера выступает L-SRV.
    b) Создайте учетные записи ldapuser1 и ldapuser2
    c) L-CLI-A, L-SRV и L-CLI-B должны аутентифицироваться через LDAP.

Конфигурация служб мониторинга,резервного копирования, журналирования

1) На L-SRV организуйте централизованный сбор журналов с хостов L-FW, L-SRV.
    d) Журналы должны храниться в директории **/opt/logs/.**
    e) Журналирование должно производится в соответствии с **Таблицей 3.**
    f) Обеспечьте ротацию логов со следующими параметрами:
        i) Размер одного файла логов не превышает 1MB
        ii) При ротации следует использовать сжатие
        iii) Обеспечьте хранение не более 5 файлов журналов

2) Разверните приложение loganalyzer на сервере L-SRV
    a) В качестве источников данных используйте собираемые логи в /opt/logs
    b) Доступ должен осуществляться по имени logs.skill39.wsr, по протоколу https.
    c) Реализуйте перенаправление http->https

Конфигурация служб удаленного доступа

1) На L-FW настройте сервер удаленного доступа на основе технологии OpenConnect
    a) Сервер должен работать на порту 4443 для tcp и udp
    b) В качестве сертификатов используйте сертификаты, выданные R-FW
    c) Разрешите исследование mtu
    d) Если клиент не активен в течении 30 минут, подключение должно быть разорвано
    e) В качестве адресного пространства для клиентов используйте 10.8.8.0/24
    f) Настройте использование DNS серверов предприятия и выдачу корректного доменного имени
    g) Все DNS запросы должны проходить через VPN туннель
    h) Сконфигурируйте пользователя vpnuser с паролем vpnpass. В качестве места хранения пользователя используйте локальную базу данных
2) На OUT-CLI настройте клиент удаленного доступа на основе технологии OpenConnect
    a) Реализуйте автоматическое подключение к VPN сервису предприятия
        i) Создайте юнит connect.service
        ii) Обеспечьте запуск юнита connect после достижения network-online.target
        iii) В качестве описания юнита задайте “VPN Connector to skill39.wsr”
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-Хеллмана — 14 (2048)

iv) Аутентификация по общему ключу WSR-2019

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

Настройка маршрутизации

5) Настройте динамическую маршрутизацию по протоколу OSPF с использованием пакета FRR:
   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.
   f) Запретите рассылку служебной информации OSPF в сторону клиентских машин и глобальной сети.

Конфигурация веб- и почтовых служб

1) На R-SRV установите и настройте веб-сервер apache:
   a) Настройте веб-сайт для внешнего пользования www.skill39.wsr.
      i) Используйте директорию **/var/www/html/out.**
      ii) Используйте порт 8088.
      iii) Сайт предоставляет доступ к двум файлам.
         1) index.html, содержимое “Hello, www.skill39.wsr is here!”
         2) date.php(исполняемый PHP-скрипт), содержимое:
            a) Вызов функции date('Y-m-d H:i:s');
2) На R-FW настройте реверс-прокси на основе NGINX:
   a) Сайт www.skill39.wsr должен быть доступен из внешней сети по внешнему адресу R-FW
   b) Все настройки, связанные с заданием, должны содержаться в отдельном конфигурационном файле в каталоге /etc/nginx/conf.d/task.conf
      i) Конфигурация основного файла должна быть минимальной и не влиять на работу NGINX в рамках выполнения задания.
   c) Настройте SSL и автоматическое перенаправление незащищенных запросов на HTTPS-порт того же самого сервера.
   d) Реализуйте пассивную проверку работоспособности бекенда.

i) Считать веб-сервер неработающим после 4 ошибок.
ii) Считать веб-сервер неработающим в течение 43 секунд.

e) Реализуйте кэширование:
i) Запросы к любым PHP-скриптам не должны кэшироваться.
ii) Кэширование успешных запросов к остальным типам данных должно выполняться в течение 40 секунд.

Конфигурация служб хранения данных

1) Преобразуйте в физические тома LVM все свободные носители.
a) Создайте группу логических томов WSR_LVM
b) Создайте следующие логические тома.
c) Users, 200 Мб.
d) Shares, 40% от оставшегося свободного места.
e) Обеспечьте создание снапшотов тома Shares раз в час.
f) Снапшоты создаются в формате SNAP-XX, где XX - номер снапшота, (01, 02 и т.д.)
g) Снапшоту выделяется 5% от общего объема группы томов.
h) Снапшоты должны создаваться при помощи скрипта /root/create_snap.sh
i) Создайте снапшот чистого тома Users с названием CLEAR
j) Снимок должен позволять хранение 30% изменений указанного логического тома.
k) Обеспечьте монтирование тома Users в каталог /opt/Users
l) Обеспечьте монтирование тома Shares в каталог /opt/Shares
m) Монтирование должно происходить во время загрузки системы.
2) Реализуйте файловый сервер на L-SRV
a) Создайте 2 общие папки shares и users
b) В папке shares создайте каталог workfolders. Внутри каталога workfolders создайте папки Work1 и Work2
i. Назначьте владельцем папки Work1 пользователя ldapuser1, владельцем папки Work2 пользователя ldapuser2
ii. Обеспечьте автоматическое монтирование каталога workfolders по протоколу smb при входе пользователя в папку work на рабочем столе
iii. Папка work должна автоматически создаваться при входе пользователя в систему и удаляться при выходе пользователя
iv. Обеспечьте отображение рабочих папок в зависимости от прав пользователя. Пользователь должен видеть только файлы и папки к которым у него есть доступ.
c) В папке users создайте домашние папки для всех пользователей LDAP
d) Обеспечьте автоматическое подключение домашних папок при входе пользователя на машины CLI1-A и CLI1-B по протоколу SMB в директорию /home

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
e) Обеспечьте автоматический импорт сертификатов из системного хранилища в браузер firefox для всех пользователей.

3) Настройте межсетевой экран **nftables** на L-FW и R-FW
   a) Создайте таблицу wsr39
   b) Создайте цепочки in_chain и out_chain для входящего и исходяшего трафика
   c) Реализуйте правила работы с трафиком
      i) Весь трафик, покидающий внутреннюю сеть должен проходить маскарадинг
      ii) Разрешите прохождение трафика, необходимого для выполнения задания
      iii) Весь остальной трафик следует запретить
4) На L-FW настройте удаленный доступ по протоколу SSH:
   a) Доступ ограничен пользователями **ssh_p, root** и **ssh_c**
      i) В качестве пароля пользователь (кроме root) использовать **ssh_pass.**
      ii) root использует стандартный пароль
   b) SSH-сервер должен работать на порту **22**
5) На OUT-CLI настройте клиент удаленного доступа SSH:
   a) Доступ к L-FW из под локальной учетной записи root под учетной записью **ssh_p** должен происходить с помощью аутентификации на основе открытых ключей.

Конфигурация и установка системы

1. На сервере R-SRV требуется выполнить обновление дистрибьютива CentOS 8. Произведите обновление ОС с использованием внешних репозиториев. Учтите, что на сервере присутствуют важные данные, по этому переустанавливать систему запрещается.

Настройка подключений к глобальным сетям

1) Настройте корректную IP-адресацию между всеми устройствами в подсети 20.20.20.0/24

Конфигурация подсистемы телефонной связи

В данном модуле настройка не предусмотрена

Виртуализация

В данном модуле настройка не предусмотрена

СУБД

В данном модуле настройка не предусмотрена

Автоматизация администрирования

В данном модуле настройка не предусмотрена

Таблица 1 – DNS-имена

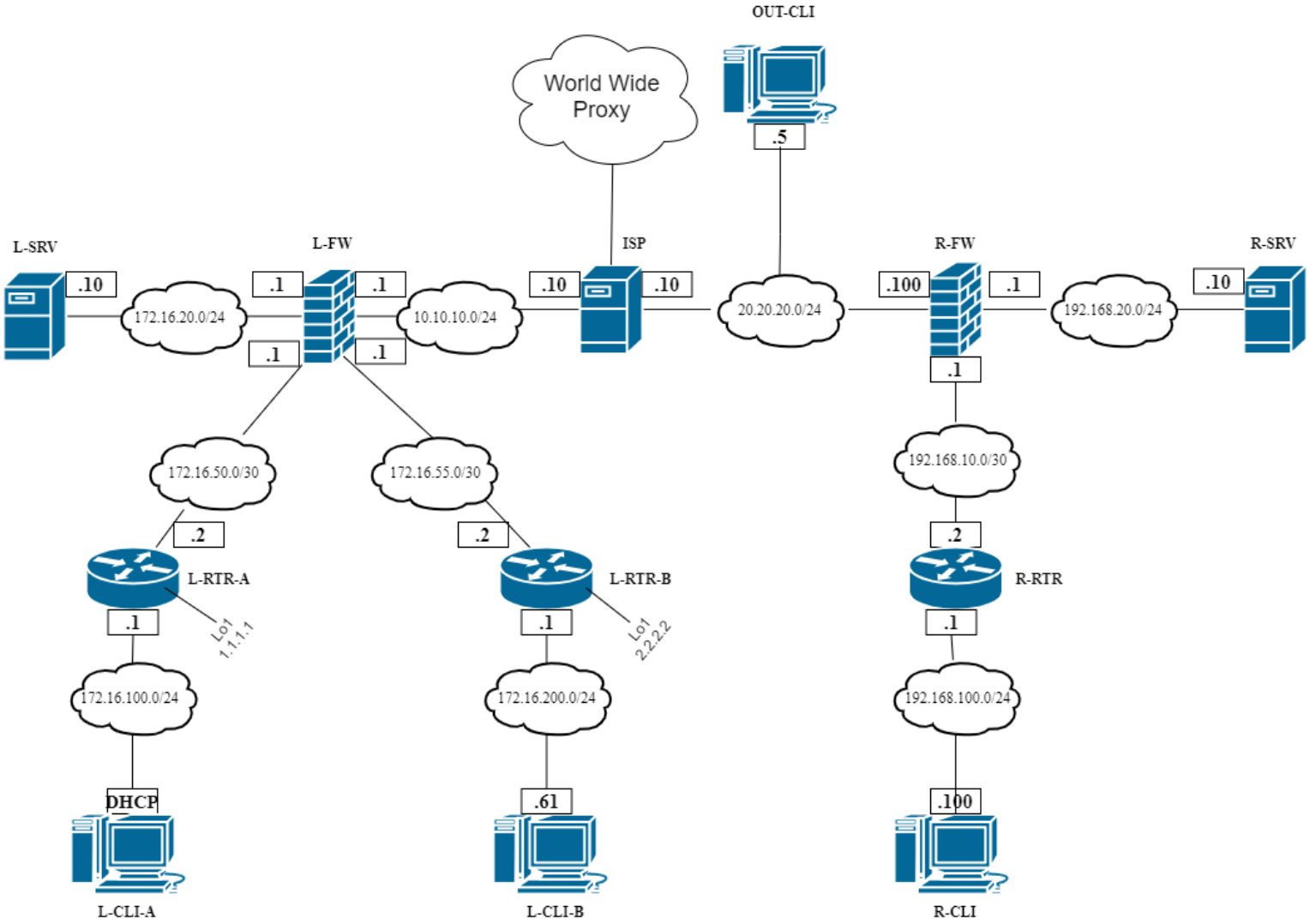
Хост	**DNS-имя**
L-CLI-A	A,PTR: l-cli-a.skill39.wsr
L-CLI-B	A,PTR: l-cli-b.skill39.wsr
L-SRV	A,PTR: l-srv.skill39.wsr CNAME: server.skill39.wsr
L-FW	A: l-fw.skill39.wsr
R-FW	A: r-fw.skill39.wsr CNAME: www.skill39.wsr
R-SRV	A,PTR: r-srv.skill39.wsr

Таблица 3 – Правила журналирования

Источник	Уровень журнала (строгое соответствие)	Файл
L-SRV	auth.*	/opt/logs/<HOSTNAME>/auth.log
L-FW	*.err	/opt/logs/<HOSTNAME>/error.log

*<HOSTNAME> - название директории для журналируемого хоста
**В директории /opt/logs/ не должно быть файлов, кроме тех, которые указаны в таблице

ДИАГРАММА ВИРТУАЛЬНОЙ СЕТИ



ВВЕДЕНИЕ

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

В рамках легенды конкурсного задания Вы – системный администратор компании, находящейся в городе Казань. В главном офисе вы управляете доменом skill39.wsr. Вам необходимо настроить сервисы в локальной сети головного офиса.

Компания, в которой вы работаете, хочет выйти на рынки северной Европы. Для этого она устанавливает партнерские отношения с одной из компаний, находящейся в Санкт-Петербурге. Вам нужно помочь администратору партнерской компании с настройкой своего домена (skill39.wsr), а потом настроить между доменами доверие.

Также Вам предстоит настроить канал связи между офисами с помощью статических маршрутов.

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

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

КОМПЛЕКТАЦИЯ КОНКУРСНОГО ЗАДАНИЯ

1. Текстовые файлы:

- данный файл с конкурсным заданием;
- файл дополнений к конкурсному заданию, содержащий: описание вида предустановок, описание используемых операционных систем, а также рекомендации по выделению ресурсов для виртуальных машин.

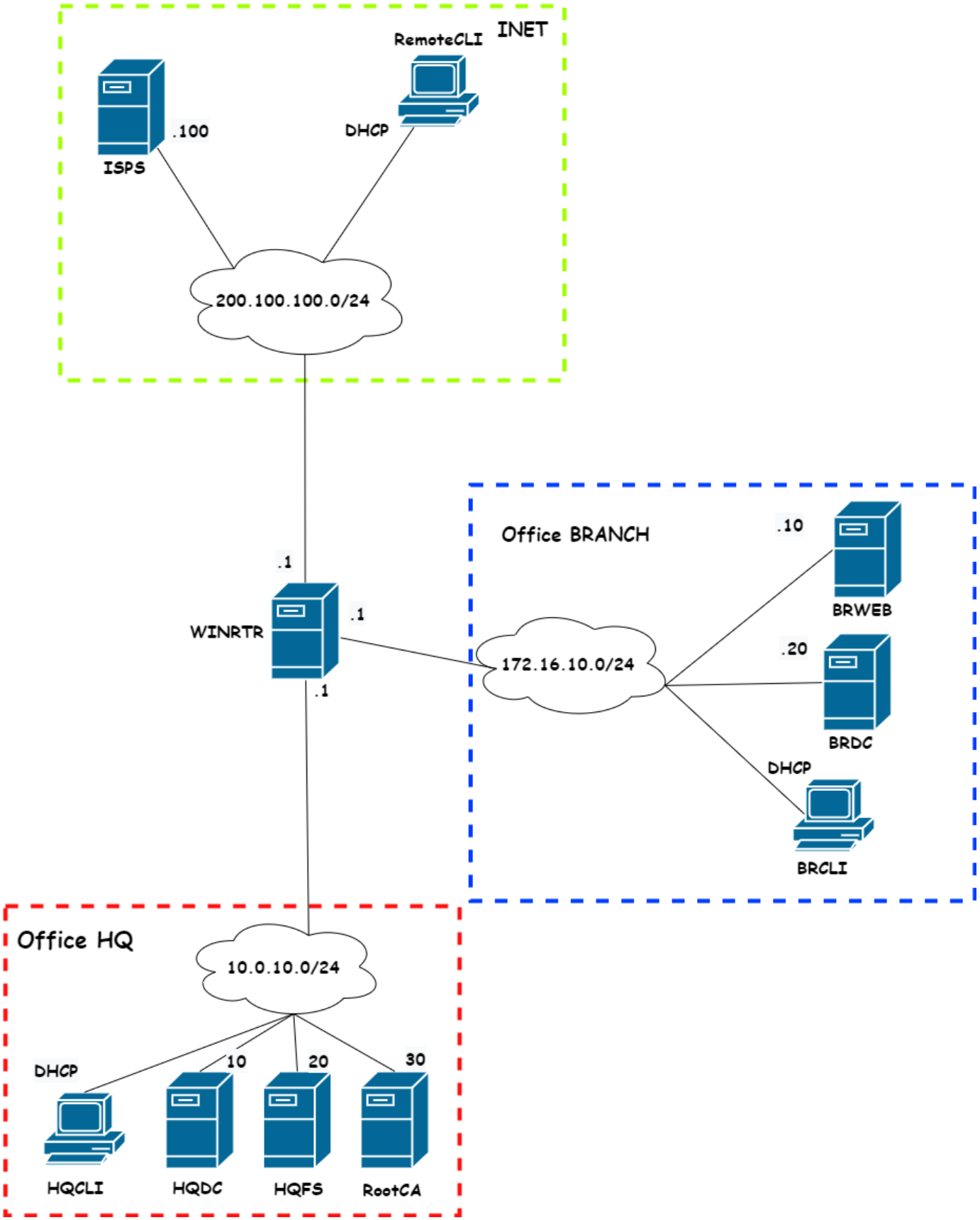
2. Программное обеспечение:

- Windows10.ADMX.

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

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

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


INET
RemoteCLI
.100
ISPS
DHCP
200.100.100.0/24
.1
WINRTR
.1
.1
Office BRANCH
.10
BRWEB
172.16.10.0/24
.20
BRDC
DHCP
BRCLI
Office HQ
10.0.10.0/24
DHCP
10
20
30
HQCLI
HQDC
HQFS
RootCA

Базовая настройка

1) Адреса и хостнеймы сконфигурированы заранее. Удостоверьтесь, что конфигурация является корректной
2) Обеспечьте возможность работы протокола icmp, windows firewall при этом должен быть включен
3) Обеспечьте ввод машин в домен
    a) В домене skill39.wsr должны присутствовать машины BRDC, BRWEB, BRCLI, HQDC, HQCLI, HQFS, RemoteCLI
    b) Остальные машины должны быть сконфигурированы для участия в рабочей группе NONDOMAIN
4) На всех машинах обоих доменов отключите режим сна
5) Проверьте работоспособность отключенного режима сна. **Без отключения режима сна проверка некоторых частей задания будет НЕВОЗМОЖНА.**

Конфигурация систем централизованного управления пользователями и компьютерами

1) На машине HQDC разверните домен skill39.wsr
    a) Импортируйте пользователей из файла C:\Users.csv при помощи скрипта C:\import_users.ps1. В скрипте могут быть допущены ошибки. Устраните ошибки в скрипте и сохраните его с названием C:\import_users_v2.ps1. Создайте организационные единицы и группы внутри. В качестве названия используйте поле Job Title пользователя. Пользователи должны располагаться в корректных организационных подразделениях и должны быть добавлены в корректные группы
    b) Для пользователей IT сконфигурируйте парольную политику со следующими параметрами:
        i) Длина пароля не менее 10 символов
        ii) Срок действия пароля 15 дней
        iii) Пароль должен быть комплексным
        iv) Парольная политика применяется только к группе IT без использования GPO
        v) Сконфигурируйте название политики ITPassPolicy
    c) Так же создайте в домене пользователя Secret с паролем P@ssw0rd. В качестве Job Title данного пользователя укажите Secret User. Пользователь должен располагаться в OU Users и не должен быть включен ни в какие группы, кроме групп по умолчанию. Так же сконфигурируйте параметр City для данного пользователя. Укажите значение Secret City
    d) Синхронизируйте время с сервером ISPS. Все остальные машины должны синхронизировать время с HQDC
    e) Поместите все клиентские машины в OU Clients, Все сервера в OU Servers. При необходимости создайте данные организационные подразделения

2) На машине BRDC разверните контроллер домена skill39.wsr только для чтения;
    a) Разрешите репликацию паролей для группы competitors
    b) Запретите репликацию паролей для группы IT и администраторов домена

3) Сконфигурируйте групповые политики в домене skill39.wsr
    a) запретите анимацию при первом входе пользователей в систему на всех клиентских компьютерах домена;
    b) члены группы IT должны быть членами группы локальных администраторов на всех клиентских компьютерах домена;
    c) Сконфигурируйте стартовую страницу www.skill39.wsr для всех клиентских машин, в браузерах Internet Explorer и Microsoft edge.
    d) **для каждого пользователя, члена группы IT, создайте автоматически подключаемую в качестве диска U:₩ домашнюю папку внутри папки по адресу SRV1→***d:\shares\IT*. Папки должны создаваться динамически, при первом входе пользователя в систему
    e) На всех клиентских компьютерах домена все пользователи должны видеть ярлык приложения калькулятор
    f) Сконфигурируйте заставку рабочего стола. Заставка должна обозначать принадлежность машины к офису, например в офисе HQ заставка должна содержать слово HQ, в офисе Branch, слово Branch.

4) Введите машину RemoteCLI в домен при помощи функции оффлайн присоединения к домену. Файл для присоединения сохраните в корне диска C:\

Конфигурация сетевой инфраструктуры

1) На сервере HQDC сконфигурируйте DHCP сервер для подсети офисов HQ и Branch
    a) в качестве диапазона выдаваемых адресов используйте все незанятые серверами адреса в подсети
    b) Обеспечьте отказоустойчивость DHCP между серверами HQDC и HQFS
        i) При выходе из строя DHCP сервера на HQDC в работу должен вступать сервер на HQFS. Все остальное время DHCP сервер на HQFS должен находится в режиме простоя
        ii) Обеспечьте автоматическое переключение между серверами не более чем за одну минуту
    c) Сконфигурируйте дополнительные опции (адреса DNS серверов и шлюз по умолчанию)

2) На машине WINRTR сконфигурируйте DHCP Relay

3) Сконфигурируйте DNS для домена skill39.wsr
    a) Обеспечьте возможность разрешения обратных имен
    b) Запретите использование нелатинских символов

c) Добавьте запись www.skill39.wsr таким образом, чтобы машины из офиса Branch обращались к BRWEB, а машины из офиса HQ к HQFS.

4) На сервере ISP сконфигурируйте эмуляцию соединения с интернетом. При проверке наличия соединения с интернетом любой сервер и любой клиент любого офиса должны давать положительный ответ. Все машины всех офисов должны считать, что они находятся в интернете

Конфигурация служб хранения данных

1) Из дополнительных жестких дисков создайте массив RAID1 и присвойте ему букву D:
2) создайте общие папки для подразделений по адресу SRV1→*d:\shares\departments.*
   a) Просматривать и редактировать файлы в папках могут только члены соответствующей группы.
3) обеспечьте привязку общей папки подразделения к соответствующей группе пользователей в качестве диска G:\.
4) пользователи домена при обращении к общим папкам, на доступ которым у них нет разрешений, должны получать вместо стандартного уведомление следующего вида: «You do not have permissions to use this path - [путь к папке]! Do not try it again!».
5) установите максимальный размер в 2 Gb для каждой домашней папки пользователя (U:\);
6) запретите хранение в домашних папках пользователей файлов с расширениями .mp3 и .wav; учтите, что файлы остальных типов пользователи вправе хранить в домашних папках.
7) для хранения профилей пользователей в домене skill39.wsr используйте общую папку по адресу HQFS→*D:\Shares\profiles;*
8) каждый пользователь должен иметь доступ к файлам только своего профиля; при обращении к указанной общей папке средствами программы *Проводник* пользователь должен видеть в списке только папку со своим профилем.
9) Создайте каталог D:\Shares\Secret. Обеспечьте возможность доступа к данному каталогу только пользователям, Job Title которых установлен как Secret User, и параметр City -- Secret City

Конфигурация веб- и почтовых служб

1) На HQFS создайте сайт www.skill39.wsr
   a) При переходе на сайт должна быть видна надпись Welcome to Head-Quater!
   b) Сайт должен быть доступен по https
      i) Используйте сертификат, выданный HQDC
      ii) При переходе на сайт не должно возникать ошибок, связанных с сертификатами

iii) Настройте автоматическое перенаправление http -> https

c) Обеспечьте возможность доступа на сайт по имени www.skill39.wsr с клиентских машин обоих офисов

2) На BRWEB создайте сайт www.skill39.wsr
   a) При переходе на сайт должна быть видна надпись Welcome to Branch!!
   b) Сайт должен быть доступен по https
      i) Используйте сертификат, выданный HQDC
      ii) При переходе на сайт не должно возникать ошибок, связанных с сертификатами
      iii) Настройте автоматическое перенаправление http -> https
   c) Обеспечьте возможность доступа на сайт по имени www.skill39.wsr с клиентских машин обоих офисов

Конфигурация параметров безопасности и служб аутентификации

1) Сконфигурируйте корневой недоменный центр сертификации на машине RootCA
   a) имя центра сертификации – HQRootCA
   b) срок действия сертификата – 8 лет;
   c) Сконфигурируйте корректные CRL и AIA
   d) Подпишите сертификат для подчиненного центра сертификации и отключите сетевой адаптер средствами операционной системы
2) Сконфигурируйте подчиненный доменный центр сертификации на машине HQDC
   a) Имя центра сертификации -- HQ Sub
   b) Срок действия 5 лет
   c) Сконфигурируйте корректные CRL и AIA
   d) Создайте шаблон для группы IT. В качестве названия шаблон укажите ITUsers, Subject Name = Common Name, обеспечьте автоматическую выдачу данного сертификата только группе IT
   e) Создайте шаблон Clients для всех клиентских компьютеров домена. В качестве названия шаблона укажите Clients, Subject Name = Common Name, обеспечьте автоматическую выдачу данного сертификата только для клиентских ПК.
3) Все машины офисов HQ и Branch должны доверять сертификатам обоих центров сертификации

Настройка маршрутизации

1) Сконфигурируйте WINRTR для достижения полной связанности между всеми офисами и интернетом.
2) Средствами Windows Firewall запретите icmp трафик из сети интернет до сети любого из офисов. Весь остальной трафик должен быть разрешен.

Конфигурация служб мониторинга,резервного копирования, журналирования
В данном модуле настройка не предусмотрена

Конфигурация служб удаленного доступа
В данном модуле настройка не предусмотрена

Настройка подключений к глобальным сетям
В данном модуле настройка не предусмотрена

Конфигурация подсистемы телефонной связи
В данном модуле настройка не предусмотрена

Виртуализация
В данном модуле настройка не предусмотрена

СУБД
В данном модуле настройка не предусмотрена

Автоматизация администрирования
В данном модуле настройка не предусмотрена

Конфигурация и установка системы
В данном модуле настройка не предусмотрена

ПРИЛОЖЕНИЕ

ВВЕДЕНИЕ. Настоящие дополнения содержат описание вида предустановок, описание используемых операционных систем, рекомендации по выделению ресурсов для виртуальных машин.

ОПИСАНИЕ ПРЕДУСТАНОВОК

1. На SRV1 должно быть установлено четыре (или пять) жестких диска: один не менее – 25 Gb, три (четыре) – 5 Gb .
2. Все остальные жесткие диски всех виртуальных машин должны иметь объем не менее 25 Gb.
3. После установки на всех виртуальных машинах необходимо выполнить сценарий *Sysprep* с опцией *generalize.*
4. После выполнения работ перезагрузка стендов остается на усмотрение экспертов.

ОПИСАНИЕ ПРИМЕНЯЕМЫХ ОПЕРАЦИОННЫХ СИСТЕМ

Имя компьютера	**Операционная система**
HQDC	Windows Server 2019 GUI
HQCLI	Windows 10 Enterprise
HQFS	Windows Server 2019 Core
BRDC	Windows 2019 GUI
ISPS	Windows 2019 GUI
RootCA	Windows Server 2019 Core
BRWEB	Windows Server 2019 Core
BRCLI	Windows 10 Enterprise
WINRTR	Windows Server 2019 GUI
RemoteCLI	Windows 10 Enterprise

Задание протестировано на 100% следующих сборках ОС:

- Server 2019 – 17763.379.190312-0539;
- Win 10 Ent – 18362.30.190401-1528.

РЕКОМЕНДАЦИИ ПО ВЫДЕЛЕНИЮ ОПЕРАТИВНОЙ ПАМЯТИ ВИРТУАЛЬНЫХ МАШИН

- Windows Server 2019 Core: минимум – 1 Gb, рекомендовано – 1,5 Gb;
- Windows Server 2019 GUI: минимум – 1,5 Gb, рекомендовано – 2 Gb;
- Windows 10 Enterprise: минимум – 1,5 Gb, рекомендовано – 2 Gb.

Модуль С: «Пусконаладка телекоммуникационного оборудования»
Версия 1 от 28.09.20

ВВЕДЕНИЕ

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

ОПИСАНИЕ КОНКУРСНОГО ЗАДАНИЯ

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

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

Все секции являются независимыми друг от друга, но вместе образуют достаточно сложную сетевую инфраструктуру. Некоторые задания достаточно просты и понятны, некоторые могут быть неочевидными. Можно заметить, что некоторые технологии должны работать в связке или поверх других технологий. Например, может подразумеваться, что IPv6 маршрутизация должна работать поверх настроенной виртуальной частной сети, которая, в свою очередь, должна работать поверх IPv4 маршрутизации, которая, в свою очередь, должна работать поверх PPPoE и Multilink и т.д. Очень важно понимать, что если вам не удается решить какую-либо из задач по середине такого технологического стека, это не значит, что решенные задачи не будут оценены. Например, если вы не можете настроить динамическую маршрутизацию IPv4, которая необходима для работы виртуальной частной сети, вы можете использовать статическую маршрутизацию и продолжать работу над настройкой виртуальной частной сети и всем что должно работать поверх нее. В этом случае вы не получите баллы за динамическую маршрутизацию, но вы получите баллы за всё что должно работать поверх нее (в случае если функциональные тесты пройдены успешно).

ИНСТРУКЦИИ ДЛЯ УЧАСТНИКА

В первую очередь необходимо прочитать задание полностью и составить алгоритм выполнения работы. Вам предстоит вносить изменения в действующую, преднастроенную сетевую инфраструктуру предприятия, состоящую из головного офиса HQ и удаленного офиса BR1. Офисы имеют связь через провайдеров ISP1 и ISP2. Вы не имеете доступа к оборудованию провайдеров, оно полностью настроено и не требует дополнительного конфигурирования. Вам необходимо настраивать оборудование предприятия, а именно: SW1, SW2, SW3, HQ1, FW1 и BR1.

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

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

PC2 Виртуальный ПК, Windows 10, Putty. Пользователь User пароль P@ssw0rd

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

1) SysLog папка для проверки /Cisco_Log
2) RADIUS - FreeRadius
3) SNMP – для проверки используется пакет Net-SNMP используйте команду snmp_test
4) NTP
5) TFTP папка для проверки /Cisco_TFTP

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

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

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

ПОДКЛЮЧЕНИЕ К УСТРОЙСТВАМ

Для подключения к FW1 используете учетную запись с логином: **cisco** и паролем: **cisco**, для входа в привилегированный режим используйте пароль **cisco**. Для подключения к остальным сетевым устройствам используйте пароль: **cisco** и пароль для привилегированного режима: **cisco**

A. Базовая настройка

1) Задайте имя всех устройств в соответствии с топологией.
2) Назначьте для всех устройств доменное имя **worldskills.ru**
3) Создайте на всех устройствах пользователей **wsruser** с паролем **network**
    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 в виде результата хэш-функции.
5) Настройте режим, при котором все пароли в конфигурации хранятся в зашифрованном виде. На FW1 используйте шифрование AES.
6) 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 удаленном подключении пользователи сразу должен получать права, соответствующие их уровню привилегий или роли (кроме межсетевого экрана FW1).
    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.
7) На устройствах, к которым разрешен доступ, в соответствии с топологиями L2 и L3, создайте виртуальные интерфейсы, подынтерфейсы и интерфейсы типа петля, назначьте IP-адреса.
8) На маршрутизаторе HQ1 на виртуальных терминальных линиях с 0 по 15 настройте аутентификацию с использованием RADIUS-сервера.
    a) Используйте на линиях vty с 0 по 15 отдельный список методов с названием method_man
    b) Порядок аутентификации:
    c) Локальная
    d) RADIUS
    e) Используйте общий ключ cisco
    f) Используйте номера портов 1812 и 1813 для аутентификации и учета соответственно
    g) Адрес RADIUS-сервера 172.16.20.20
    h) Настройте авторизацию при успешной аутентификации
    i) Проверьте аутентификацию по протоколу RADIUS при удаленном подключении к маршрутизатору HQ1, используя учетную запись **radius** с паролем **cisco**

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

B. Настройка коммутации

1) Создайте таблицу VLAN:
    i) VLAN1000 с именем **MGT**.
    ii) VLAN1200 с именем **DATA**.
    iii) VLAN1300 с именем **OFFICE**.
    iv) VLAN1500 с именем **NATIVE**.
    v) VLAN1600 с именем **SHUTDOWN**.

2) Отключите протокол VTP явным образом
3) Между всеми коммутаторами настройте транки с использованием протокола IEEE 802.1q.
    a) Порты F0/10 коммутаторов SW2 и SW3, а также порт F0/1 коммутатора SW1 должны работать без использования согласования. Отключите протокол DTP явным образом.
    b) Транк между коммутаторами SW2 и SW3 должен быть настроен без использования согласования. Отключите протокол DTP явным образом.
    c) 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.
    d) Для всех магистральных каналов назначьте native vlan 500.
    e) Запретите пересылку по магистральным каналам все неиспользуемые VLAN, в том числе VLAN1
4) Настройте агрегирование каналов связи между коммутаторами.
    a) Номера портовых групп:

1 – между коммутаторами SW1 (F0/5-6) и SW2 (F0/5-6);
2 – между коммутаторами SW1 (F0/3-4) и SW3 (F0/3-4);

    b) Агрегированный канал между SW1 и SW2 должен быть организован с использованием протокола согласования LACP. SW1 должен быть настроен в активном режиме, SW2 в пассивном.
    c) Агрегированный канал между SW1 и SW3 должен быть организован с использованием протокола согласования PAgP. SW1 должен быть настроен в предпочтительном, SW3 в автоматическом.
5) Конфигурация протокола остовного дерева:
    a) Используйте протокол MST.
    b) Сконфигурируйте имя региона WSR39
    c) Сконфигурируйте 2 инстанса
        a. 1 - VLAN100, VLAN1200,VLAN1300
        b. 2 - VLAN 1500, VLAN 1600

d) В качестве корневого коммутатора для 1 инстанса сконфигурируйте SW1
e) В качестве корневого коммутатора для 2 инстанса сконфигурируйте SW2
f) Обеспечьте быстрое согласование магистральных каналов (Без ожидания MSTP)

6) Настройте порты F0/10 коммутаторов SW2 и SW3 в соответствии с L2 диаграммой.
7) Между HQ1 и FW1 настройте взаимодействие по протоколу IEEE 802.1Q.
8) На всех устройствах, отключите неиспользуемые порты.
9) На всех коммутаторах, неиспользуемые порты переведите во VLAN 1600.

C. Настройка подключений к глобальным сетям

1) Подключение FW1 к ISP1 и ISP2 осуществляется с помощью IPoE, настройте интерфейсы в соответствии с диаграммами L2 и L3.
   a) Передача данных между FW1 и ISP1 осуществляется не тегированным трафиком.
   b) Передача данных между FW1 и ISP2 осуществляется тегированным трафиком с использованием VLAN 901.
2) ISP3 предоставляет L2 VPN между офисами HQ и BR1.
   a) Настройте передачу между HQ1, FW1 и BR1 тегированного трафика.

   В зависимости от используемой модели межсетевого экрана, выберите один из двух следующих пунктов задания:

   Для ASA5505:

   b) Взаимодействие должно осуществляться по VLAN 10.

   Для ASA5506:

   b) Для обеспечения L2 связности между маршрутизатором BR1 и маршрутизатором HQ1, на межсетевом экране FW1 используйте Bridge group Virtual Interface (BVI) под номером 2. Для этого на межсетевом экране добавьте в BVI2, два подинтерфейса: с тегом 10 в сторону провайдера ISP3, с тегом 11 в сторону маршрутизатора HQ1. На маршрутизаторе HQ1 в сторону межсетевого экрана FW1, создайте соответствующий подинтерфейс.
3) Настройте подключение BR1 к провайдеру ISP1 с помощью протокола PPP.
   a) Настройте Multilink PPP с использованием двух Serial-интерфейсов.
   b) Используйте 1 номер интерфейса.
   c) Не используйте аутентификацию.
   d) BR1 должен автоматически получать адрес от ISP1.
4) Настройте подключение BR1 к провайдеру ISP2 с помощью протокола HDLC.

D. Настройка маршрутизации

ВАЖНО! При настройке протоколов динамической маршрутизации, будьте предельно внимательны и анонсируйте подсети в соответствии с диаграммой маршрутизации, иначе не получите баллы за протокол, в котором отсутствует

необходимая подсеть, и за тот протокол, в котором эта подсеть оказалась лишней.
Также, стоит учесть, что провайдеры фильтруют маршруты полученные по BGP, если они не соответствуют диаграмме маршрутизации.

1) В офисе HQ, на устройствах HQ1 и FW1 настройте протокол динамической маршрутизации OSPF.
   a) Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
   b) HQ1 и FW1 между собой должны устанавливать соседство, только в сети 172.16.3.0/24.
   c) 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.
   a) Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
   b) Используйте магистральную область для GRE туннелей.
   c) Соседства между офисами HQ и BR1 должны устанавливаться, как через канал L2 VPN, так и через защищенный туннель.
   d) Убедитесь в том, что при отказе выделенного L2 VPN, трафик между офисами будет передаваться через защищённый GRE туннель.
   e) Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.
3) Настройте протокол BGP в офисах HQ и BR1 для взаимодействия с провайдерами ISP1 и ISP2.
   a) На устройствах настройте протокол динамической маршрутизации BGP в соответствии с таблицей 1

Таблица 1 – BGP AS

Устройство	AS
HQ1	65000
FW1	65000
ISP1	65001
ISP2	65002
BR1	65010

   b) Настройте автономные системы в соответствии с Routing-диаграммой.
   c) Маршрутизаторы HQ1 и FW1 должны быть связаны с помощью iBGP. Используйте для этого соседства, интерфейсы, которые находятся в подсети 30.78.87.0/29.

d) Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
e) Для офиса BR исключите из таблицы маршрутизации сеть 14.88.22.8

4) Настройте протокол динамической маршрутизации EIGRP поверх защищенного туннеля и выделенного канала L2 VPN между маршрутизаторами HQ1 и BR1.
a) Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
b) Используйте номер автономной системы 6000.

E. Настройка служб

1) В сетевой инфраструктуре сервером синхронизации времени является SRV1. Все остальные сетевые устройства должны использовать его в качестве сервера времени.
a) Передача данных между осуществляется без аутентификации.
b) Настройте временную зону с названием MSK, укажите разницу с UTC +3 часов.
2) Настройте динамическую трансляцию портов (PAT):
a) На маршрутизаторе HQ1 и BR1 настройте динамическую трансляцию портов (PAT) для сети 192.168.2.0/24 в соответствующие адреса петлевых интерфейсов.
b) Убедитесь в том, что для PC2 для выхода в интернет использует один из каналов до ISP1 или ISP2 от BR1, при недоступности обоих каналов, PC2 должен осуществлять выход в сеть интернет через каналы офиса HQ.
c) Убедитесь, в том, что есть все необходимые маршруты, иначе проверить корректность настроенной трансляции портов, будет невозможно.

3) Настройте протокол динамической конфигурации хостов со следующими характеристиками
a. На маршрутизаторе HQ1 для подсети OFFICE:
i) Адрес сети – 30.78.21.0/24.
ii) Адрес шлюза по умолчанию интерфейс роутера HQ1.
iii) Адрес NTP-сервера 172.16.20.20.
iv) Компьютер PC1 должен получать адрес 30.78.21.10.

4) В офисе BR1 используется аутентификация клиентов с помощью протокола L2TP. Для этого настройте сервер L2TP на BR1.
c) Аутентификация PC2 на сервере L2TP должна осуществляться по логину pc2user и паролю pc2pass.
d) PC2 должен получать ip адрес от L2TP сервера автоматически.
e) В качестве транспортного адреса используте адреса из подсети 192.168.2.0/24
f) В качестве туннельных адресов используйте подсеть 10.8.8.0/24

F. Настройка механизмов безопасности

1) На маршрутизаторе BR1 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, а также включать и отключать отладку с помощью команд **debug**.
    c) Создайте и назначьте view-контекст **sh_view** на пользователя **user2**
        i) Команду show cdp neighbor
        ii) Все команды show ip *
        i) Команду ping
        ii) Команду traceroute
    d) Убедитесь, что пользователи не могут выполнять другие команды в рамках присвоенных контекстов и уровней привилегий.
2) На порту F0/10 коммутатора SW2, включите и настройте Port Security со следующими параметрами:
    a) не более 2 адресов на интерфейсе
    b) адреса должны динамически определяться, и 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 порту f0/10 коммутатора SW2 реализуйте защиту от перехвата трафика между двумя узлами в одном широковещательном домене
4) На коммутаторе SW2 включите DHCP Snooping для подсети OFFICE. Используйте флеш-память в качестве места хранения базы данных.
5) На коммутаторе SW2 включите динамическую проверку ARP-запросов в сети OFFICE.
6) На маршрутизаторе BR1 настройте расширенный список контроля доступа для подсети 192.168.2.0/24. Заблокируйте весь исходящий и входящий трафик от подсети 192.168.2.0/24 в интернет за исключением:
    a) Разрешите работу с DNS сервером 8.8.8.8.
    b) Разрешите исходящий TCP трафик по портам 80 и 443.
    c) Разрешите входящий трафик по TCP, только для тех соединений, если узел из подсети 192.168.2.0/24 инициирует это соединение.

G. Настройка параметров мониторинга и резервного копирования

1) На маршрутизаторе HQ1 и межсетевом экране FW1 настройте журналирование системных сообщений на сервер SRV1, включая информационные сообщения.
2) На маршрутизаторе HQ1 и межсетевом экране FW1 настройте возможность удаленного мониторинга по протоколу SNMP v3.

a) Задайте местоположение устройств MSK, Russia
b) Задайте контакт admin@wsr.ru
c) Используйте имя группы WSR.
d) Создайте профиль только для чтения с именем RO.
e) Используйте для защиты SNMP шифрование AES128 и аутентификацию SHA1.
f) Используйте имя пользователя: **snmpuser** и пароль: **snmppass**
g) Для проверки вы можете использовать команду snmp_test на SRV1.

3) На маршрутизаторе HQ1 настройте резервное копирование конфигурации
   a) Резервная копия конфигурации должна сохраняться на сервер SRV1 по протоколу TFTP при каждом сохранении конфигурации в памяти устройства
   b) Для названия файла резервной копии используйте шаблон <hostname>-<time>.cfg
4) На маршрутизаторе BR1 настройте мониторинг качества связи канала PPP к ISP1
   a) При качестве пропускной способности ниже 70% порт должен автоматически отключаться, а трафик перестраивается на резервный канал связи

H. Конфигурация виртуальных частных сетей

1) Между HQ1 и BR1 настройте GRE туннель со следующими параметрами:
   a) Используйте в качестве VTI интерфейс Tunnel1
   b) Используйте адресацию в соответствии с L3-диаграммой
   c) Режим — GRE multipoint
   d) HQ1 является хабом
   e) Параметры NHRP сконфигурируйте по своему усмотрению
   f) Интерфейс-источник — Loopback-интерфейс на каждом маршрутизаторе.
   g) Обеспечьте работу туннеля с обеих сторон через провайдера ISP1

2) Защита туннеля должна обеспечиваться с помощью IPsec между BR1 и FW1.
   a) Обеспечьте шифрование только GRE трафика.
   b) Используйте аутентификацию по общему ключу.
   c) Параметры IPsec произвольные.

Конфигурация подсистемы телефонной связи

1) На маршрутизаторе HQ1 сконфигурируйте CME со следующими параметрами
   a) Зарегистрируйте программный телефон на PC1 с номером 104
   b) Зарегистрируйте программный телефон на PC2 с номером 107
   c) Обеспечьте возможность звонков с одного телефона на другой
   d) Произведите необходимые настройки BR1 для регистрации телефона на PC2 в HQ CME

Конфигурация служб удаленного доступа
В данном модуле настройка не предусмотрена

Конфигурация веб- и почтовых служб
В данном модуле настройка не предусмотрена

Конфигурация служб хранения данных
В данном модуле настройка не предусмотрена
Виртуализация
В данном модуле настройка не предусмотрена

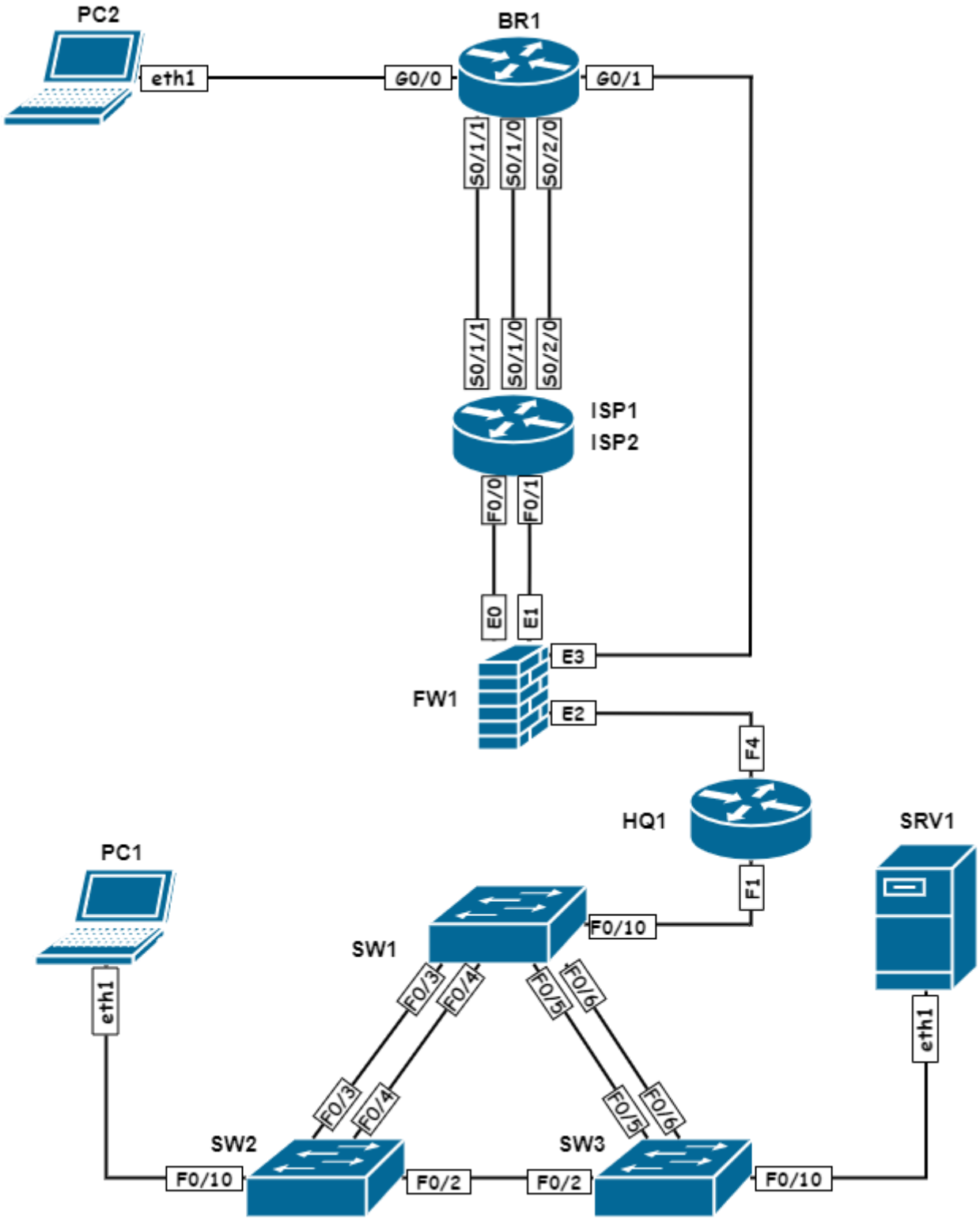
СУБД
В данном модуле настройка не предусмотрена

Конфигурация систем централизованного управления пользователями и компьютерами
В данном модуле настройка не предусмотрена

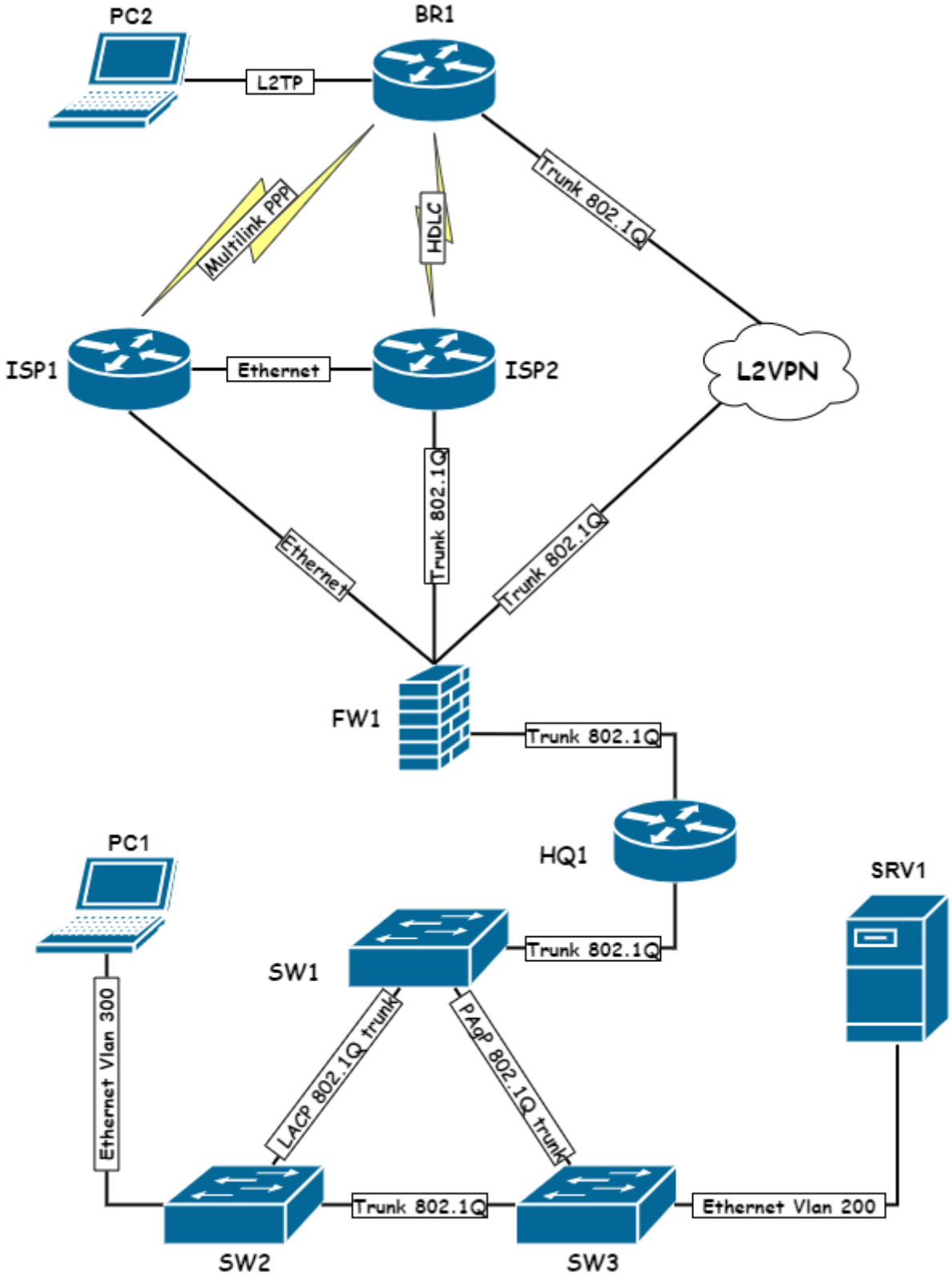
Автоматизация администрирования
В данном модуле настройка не предусмотрена

Конфигурация и установка системы
В данном модуле настройка не предусмотрена

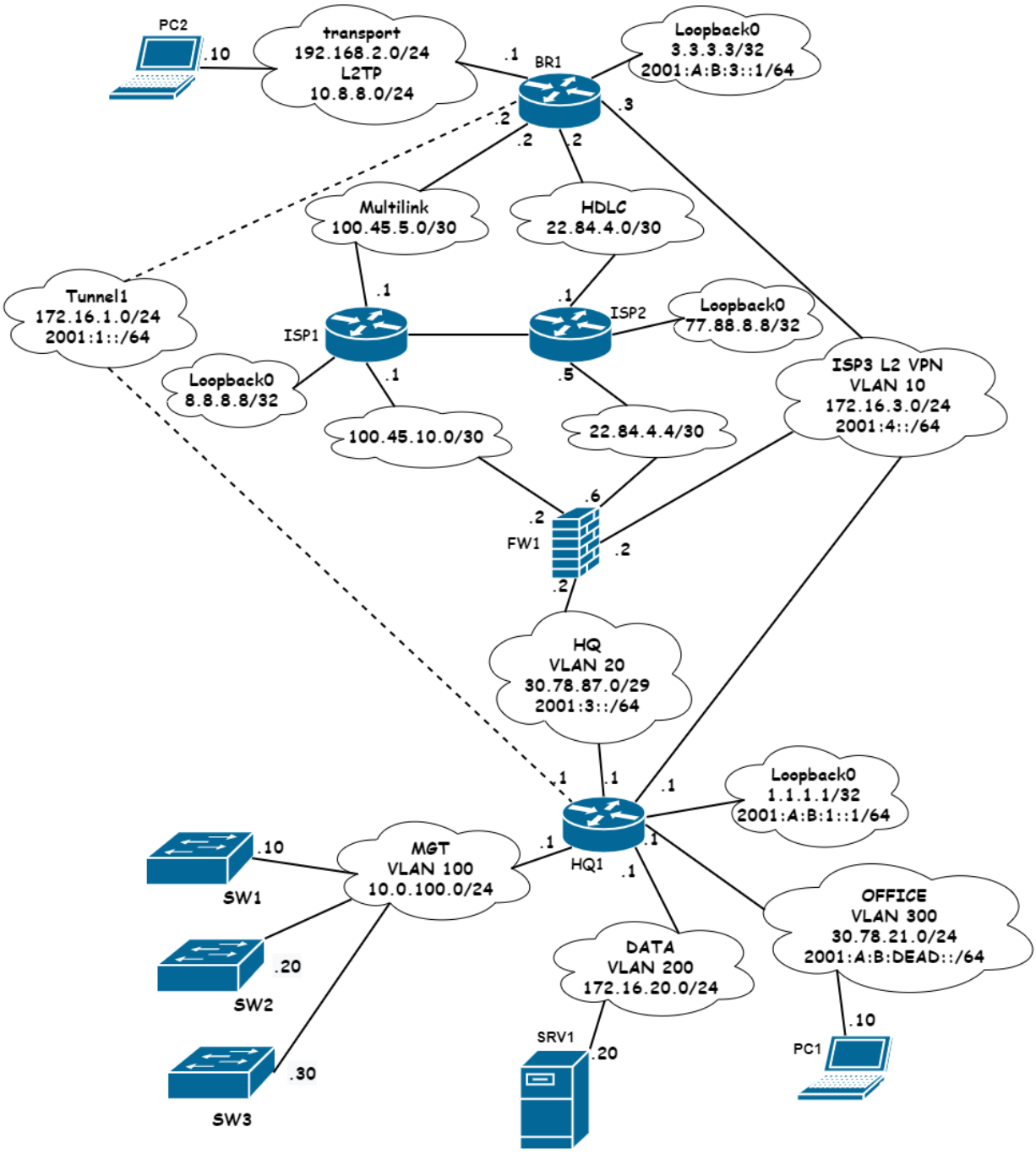
Топология L1



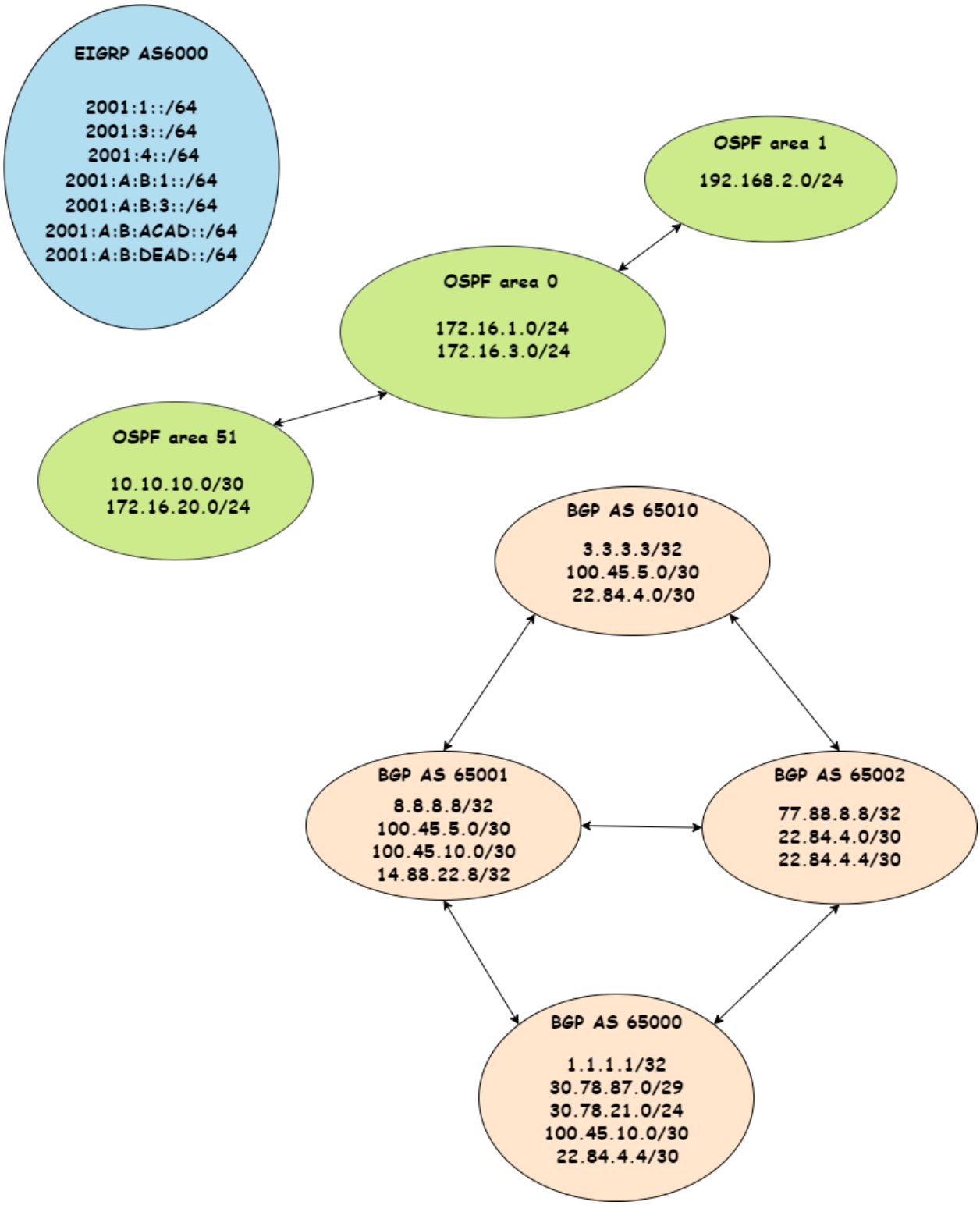
Топология L2



Топология L3



Routing-диаграмма


EIGRP AS6000
2001:1::/64
2001:3::/64
2001:4::/64
2001:A:B:1::/64
2001:A:B:3::/64
2001:A:B:ACAD::/64
2001:A:B:DEAD::/64
OSPF area 1
192.168.2.0/24
OSPF area 0
172.16.1.0/24
172.16.3.0/24
OSPF area 51
10.10.10.0/30
172.16.20.0/24
BGP AS 65010
3.3.3.3/32
100.45.5.0/30
22.84.4.0/30
BGP AS 65001
8.8.8.8/32
100.45.5.0/30
100.45.10.0/30
14.88.22.8/32
BGP AS 65002
77.88.8.8/32
22.84.4.0/30
22.84.4.4/30
BGP AS 65000
1.1.1.1/32
30.78.87.0/29
30.78.21.0/24
100.45.10.0/30
22.84.4.4/30

4. КРИТЕРИИ ОЦЕНКИ

В данном разделе определены критерии оценки и количество начисляемых баллов (субъективные и объективные) таблица 2. Общее количество баллов задания/модуля по всем критериям оценки составляет 45.

Таблица 2 – Критерии оценки

Раздел	Критерий	Оценки		
		Субъективная (если это применимо)	Объективная	Общая
A	Модуль A: «Пусконаладка инфраструктуры на основе ОС семейства Linux»	0	15	15
B	Модуль B: «Пусконаладка инфраструктуры на основе ОС семейства Windows»	0	15	15
C	Модуль C: «Пусконаладка телекоммуникационного оборудования»	0	15	15
Итого =		0	45	45

5. Приложения к заданию

5.1 Предварительные настройки модуля А

1. На всех виртуальных машинах предустановлены пакеты bind-utils, net-tools, traceroute