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.

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
Модуль B: «Пусконаладка инфраструктуры на основе ОС семейства Windows»	Ведущий разработчик	Д.В. Дюгуров
Модуль C: «Пусконаладка телекоммуникационного оборудования»	Ведущий разработчик	С.И. Добрынин
	Группа разработки	А.А. Щербинин
	Группа разработки	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 A: «Пусконаладка инфраструктуры на основе ОС семейства Linux»	В соответствии с жеребьевкой по циклу A-B-C	5 ч.
2	Модуль B: «Пусконаладка инфраструктуры на основе ОС семейства Windows»		5 ч.
3	Модуль C: «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 **Debian**

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

Вам доступен диск CentOS-7-x86_64-Everything-1810.iso

Вам доступен диск debian-10.0.0-amd64-BD-1.iso

Вам доступен диск debian-10.0.0-amd64-BD-2.iso

Вам доступен диск debian-10.0.0-amd64-BD-3.iso

Вам доступен диск debian-10.0.0-amd64-BD-4.iso

Вам доступен диск Additional.iso, на котором располагаются недостающие RPM пакеты

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

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

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

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

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.

Конфигурация хостов

1) Настройте имена хостов в соответствии с **Диаграммой.**
2) Установите следующее ПО на **ВСЕ** виртуальные машины:
    a) tcpdump
    b) net-tools
    c) curl
    d) vim
    e) lynx
    f) dhclient
    g) bind-utils
    h) nfs-utils
    i) cifs-utils
    j) sshpass
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.
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.

Службы централизованного управления и журналирования

1) Разверните LDAP-сервер для организации централизованного управления учетными записями
   a) В качестве сервера выступает L-SRV.
   b) Учетные записи создать в соответствии с **Таблицей 2**.
   c) Группы(LDAP) 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-CLI-A, L-SRV и L-CLI-B должны аутентифицироваться через LDAP.
2) На L-SRV организуйте централизованный сбор журналов с хостов L-FW, L-SRV.
   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.**
   f) Подключившийся клиент должен быть автоматически сконфигурирован на использование DNS-инфраструктуры предприятия.
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.
      iv) Используйте следующий каталог для расположения файлов скриптов **/opt/vpn/.**
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
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.
6) 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**
7) 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 веб-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) Реализуйте синхронизацию каталогов на основе демона rsyncd.
   a) В качестве сервера синхронизации используется L-SRV.
      i. Для работы синхронизации создайте специального пользователя mrsync
         1. В качестве пароля используйте toor.
      ii. Домашний каталог данного пользователя должен быть расположен в /opt/sync/. Данный каталог используйте как каталог синхронизации
      iii. Домашний каталог не должен содержать никакой посторонней информации.
      iv. Для выполнения синхронизации создайте rsync-пользователя sync с паролем parol666.
      v. Подключение к rsyncd должны быть разрешены исключительно от клиентов L-CLI-A и L-CLI-B
   b) В качестве клиентов используются L-CLI-A и L-CLI-B
      i. Синхронизируемый каталог располагается по адресу /root/sync/
      ii. Каталоги должны быть зеркально идентичны по содержимому.
         1. Приоритетным каталогом считается каталог на L-CLI-A
      iii. Реализуйте синхронизацию в виде скрипта:
         1. Скрипт находится по адресу /root/sync.sh
         2. Автоматизация скрипта реализована средствами cron пользователя root.
         3. Выполнение производится каждую минуту.

Конфигурация параметров безопасности и служб аутентификации

1) Настройте CA на R-FW, используя OpenSSL.
   a) Используйте **/etc/ca** в качестве корневой директории CA
   b) Атрибуты CA должны быть следующими:
      i) Страна RU
      ii) Организация WorldSkills Russia
      iii) CN должен быть установлен как WSR CA
   c) Создайте корневой сертификат CA
   d) Все клиентские операционные системы должны доверять CA
3) Настройте межсетевой экран **iptables** на L-FW и **firewalld** на 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 для работы настроенных сервисов.
   g) 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-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 2 – Учетные записи LDAP

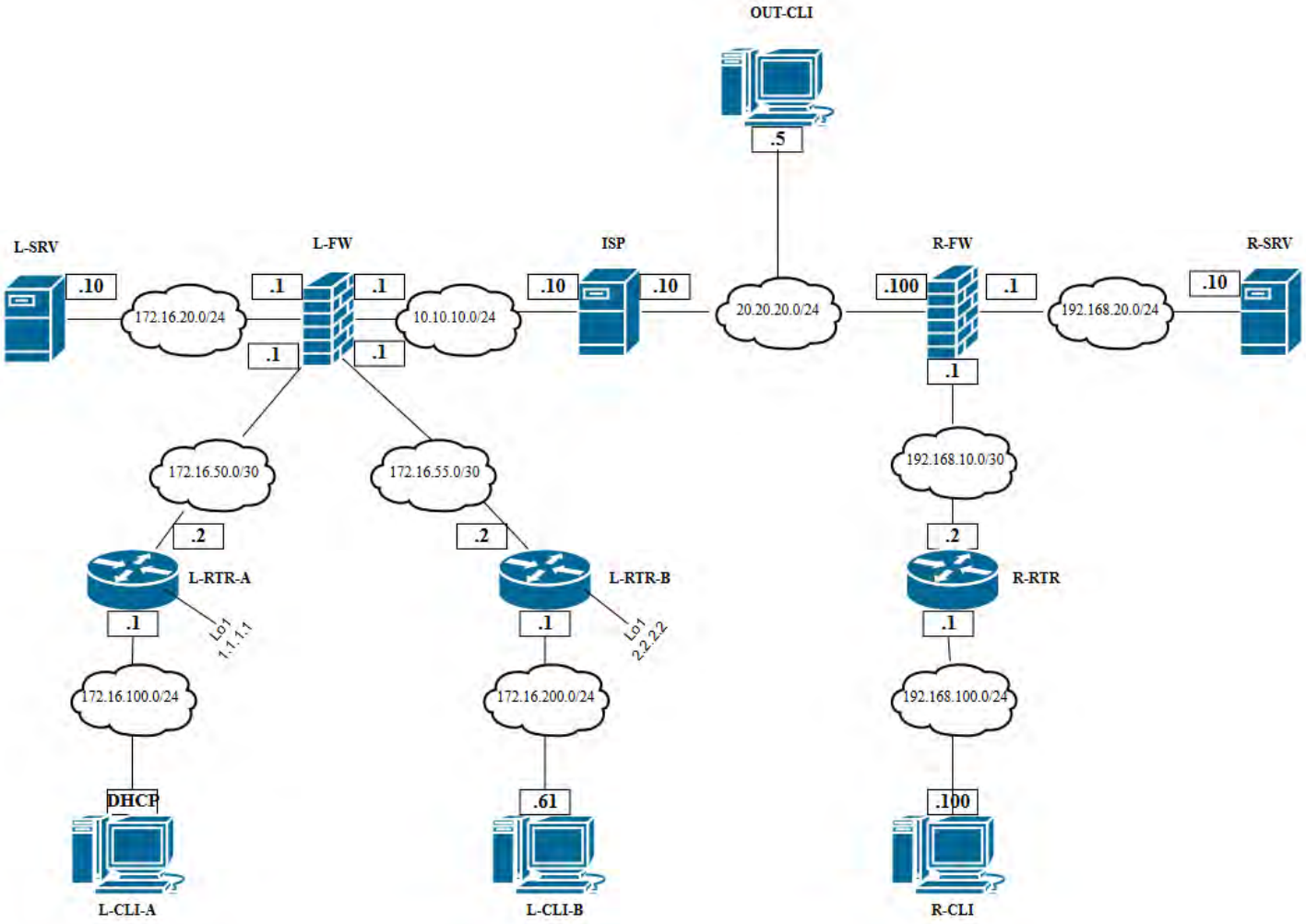
Группа	**CN**	**Пароль**	**Доступ**
Admin	tux	toor	L-SRV, L-CLI-A L-CLI-B
Guest	user1 – user99	P@ssw0rd	L-CLI-A L-CLI-B

Таблица 3 – Правила журналирования

Источник	Уровень журнала (строгое соответствие)	Файл
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 Kazan.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 (SPB.wse), 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:

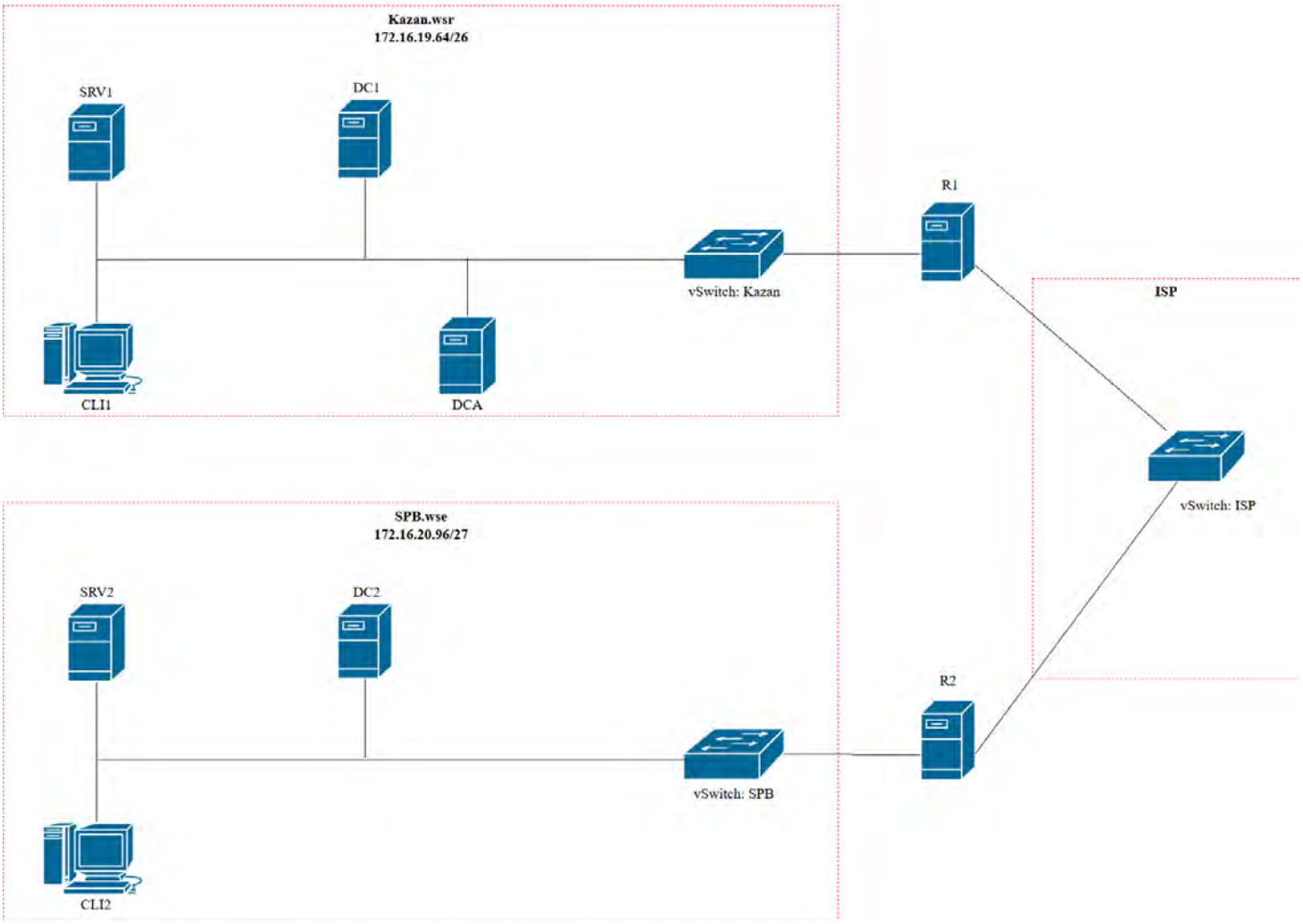
- Windows10.ADMX.

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.

Network diagram



Настройка DC1

Базовая настройка

- переименуйте компьютер в DC1;
- в качестве адреса DC1 используйте первый возможный адрес из подсети 172.16.19.64/26;
- обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей.

Active Directory

- сделайте сервер контроллером домена Kazan.wsr.

DHCP

- настройте протокол DHCP для автоконфигурации клиентов – в качестве диапазона выдаваемых адресов используйте все незанятые серверами адреса в подсети;
- настройте failover: mode – Load balancer, partner server – SRV1, state switchover – 5 min;
- настройте дополнительные свойства области (адреса DNS-серверов и основного шлюза).

DNS

- настройте необходимые зоны прямого и обратного просмотра;
- создайте все необходимые записи типа A и PTR для серверов домена и необходимых web-сервисов;
- обеспечьте разрешение имен сайтов обеих компаний.

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 должна быть настроена стартовая страница – www.kazan.wsr;
- 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!».

Элементы доменной инфраструктуры

- создайте подразделения: IT и Sales;
- в соответствующих подразделениях создайте одноименные доменные группы.
- в каждой группе создайте с помощью скрипта по 30 пользователей. Все учетные записи должны иметь возможность входа в домен с логином, созданным по следующему шаблону *НазваниеГруппы_ПорядковыйНомерПользователя@kazan.wsr*.

Пароли должны быть созданы по следующему шаблону: *НазваниеГруппы_ПорядковыйНомерПользователя*, но записанному наоборот (справа-налево). Все учетные записи пользователей должны быть включены. Вход в систему должен быть обеспечен для всех пользователей со всех клиентских компьютеров домена и рядовых серверов.

- для каждого пользователя, члена группы IT, создайте автоматически подключаемую в качестве диска U:₩ домашнюю папку внутри папки по адресу SRV1→*d:\shares\IT*;
- все пользователи при первом входе в домен с компьютера CLI1 должны видеть на рабочем столе ярлык программы *Калькулятор*.

Настройка SRV1

Базовая настройка

- переименуйте компьютер в SRV1;
- в качестве адреса SRV1 используйте второй возможный адрес из подсети 172.16.19.64/26;
- обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей.
- с помощью дополнительных жестких дисков создайте RAID-5 массив; назначьте ему букву D:\.

Active Directory

- сделайте сервер дополнительным контроллером домена Kazan.wsr;
- сервер должен быть контроллером домена только для чтения.

DHCP

- настройте протокол DHCP для автоконфигурации клиентов;
- настройте failover: mode – Load balancer, partner server – DC1, state switchover – 5 min.

DNS

- сделайте сервер дополнительным DNS-сервером в домене Kazan.wsr;
- загрузите с DC1 все зоны прямого и обратного просмотра;
- на SRV1 не должно быть основных зон, связанных с доменом Kazan.wsr и сетью 172.16.19.64.

Общие папки

- создайте общие папки для подразделений (IT, Sales) по адресу SRV1→*d:\shares\departments*. Просматривать и редактировать файлы в папках могут только члены соответствующей группы.

- обеспечьте привязку общей папки подразделения к соответствующей группе пользователей в качестве диска G:\.

Квоты/Файловые экраны

- установите максимальный размер в 2 Gb 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 компании со стартовой страницей следующего содержания:

```
<html>
    Welcome to Kazan!
</html>;
```

- сайт должен быть доступен по именам www.kazan.wsr и kazan.wsr только по протоколу https в обоих сетевых сегментах с использованием сертификатов, выданных DCA.

Настройка DCA

Базовая настройка

- переименуйте компьютер в DCA;
- в качестве адреса DCA используйте третий возможный адрес из подсети 172.16.19.64/26;
- обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей;
- присоедините компьютер к домену Kazan.wsr.

Службы сертификации

- установите службы сертификации;
- настройте основной доменный центр сертификации;
- имя центра сертификации – RootKazanCA;
- срок действия сертификата – 8 лет;
- настройте шаблон выдаваемого сертификата для клиентских компьютеров ClientComps: subject name=common name, автозапрос только для компьютера R1;
- настройте шаблон выдаваемого сертификата *ITUsers*: *subject name=common name*, автозапрос только для пользователей – членов группы IT.

Настройка CLI1

Базовая настройка

- переименуйте компьютер в CLI1;
- обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей;
- присоедините компьютер к домену *Kazan.wsr;*
- 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 *Kazan.wsr:* пользователей, общих папок, групповых политик.

Настройка DC2

Базовая настройка

- переименуйте компьютер в DC2;
- в качестве адреса DC2 используйте первый возможный адрес из подсети 172.16.20.96/27;
- обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей.

Active Directory

- сделайте сервер контроллером домена *SPB.wse;*
- настройте двустороннее доверие доменом *Kazan.wsr.*

DHCP

- настройте протокол DHCP для автоконфигурации клиентов – в качестве диапазона выдаваемых адресов используйте все незанятые 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 обеих компаний.

Элементы доменной инфраструктуры

- создайте учетную запись пользователя домена *User1\P@ssw0rd*, используйте группу по умолчанию – *Domain Users*.
- для всех пользовательских учетных записей в домене используйте перемещаемые профили;
- для хранения профилей пользователей используйте общую папку по адресу SRV2→*c:\profiles;*
- 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.

GPO

- настройте необходимые политики, обеспечивающие использование сервера DCA.kazan.wsr в качестве доверенного центра сертификации.

Настройка SRV2

Базовая настройка

- переименуйте компьютер в SRV2;
- в качестве адреса SRV1 используйте второй возможный адрес из подсети 172.16.20.96/27;
- обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей;
- присоедините компьютер к домену *SPB.wse.*

IIS

- создайте сайт компании со стартовой страницей следующего содержания:

  <html>
  Welcome to Saint-Petersburg!
  </html>;
- сайт должен быть доступен по именам *www.spb.wse* и *spb.wse* только по протоколу https в обоих сетевых сегментах с использованием сертификатов, выданных DCA.

Настройка CLI2

Базовая настройка

- переименуйте компьютер в CLI2;
- обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей;
- присоедините компьютер к домену *SPB.wse.*
- 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 *SPB.wse.*

Настройка R2

Базовая настройка

- переименуйте компьютер в R2;
- задайте настройки сети следующим образом: для сетевого интерфейса, подключенного к коммутатору ISP, используйте адрес 200.100.100.1/30; для сетевого адреса в подсети *SPB.wse* используйте последний возможный адрес из используемого адресного пространства;
- обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей;
- присоедините компьютер к домену *SPB.wse.*

Настройка RRAS

- установите службу RRAS;
- настройте статические маршруты для связи с сетевым сегментом в Казани.

Настройка R1

Базовая настройка

- переименуйте компьютер в R1;
- задайте настройки сети следующим образом: для сетевого интерфейса, подключенного к подключенного к коммутатору ISP, используйте адрес 200.100.100.2/30; для сетевого адреса в подсети Kazan.wsr используйте последний возможный адрес из используемого адресного пространства;
- обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей;
- присоедините компьютер к домену Kazan.wsr.

Настройка RRAS

- установите службу RRAS;
- настройте статические маршруты для связи с сетевым сегментом в Санкт-Петербурге.

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**
DC2	Windows Server 2019 GUI
CLI2	Windows 10 Enterprise
SRV2	Windows Server 2019 Core
R2	Windows 2019 GUI
DC1	Windows 2019 GUI
SRV1	Windows Server 2019 Core
R1	Windows Server 2019 Core
CLI1	Windows 10 Enterprise
DCA	Windows Server 2019 GUI

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.

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 первоначального подключения используйте протокол Telnet. 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**

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

SW1 – **192.168.254.10**
SW2 – **192.168.254.20**
SW3 – **192.168.254.30**
HQ1 – **192.168.254.1**
FW1 – **192.168.254.2**
BR1 – **192.168.254.3**

ОЦЕНКА

Оценка осуществляется по SSH или Telnet с устройства PC1. Проверочная группа не осуществляет перекоммутацию на стенде, поэтому будьте предельно внимательны, перед завершением выполнения конкурсного задания и верните коммутацию в исходное состояние. А также убедитесь, что устройства доступны по следующим адресам, по SSH или Telnet с учетными записями соответствующим конкурсному заданию:

SW1 – **10.100.100.10** или **192.168.254.10**
SW2 – **10.100.100.20** или **192.168.254.20**
SW3 – **10.100.100.30** или **192.168.254.30**
HQ1 – **30.78.21.1** или **192.168.254.1**
FW1 – **30.78.87.2** или **192.168.254.2**
BR1 – **172.16.3.3** или **172.16.1.2** или **3.3.3.3** или **192.168.254.3**

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 удалённом 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) По протоколу RADIUS
    d) Локальная
    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) Для централизованного конфигурирования VLAN в коммутируемой сети предприятия используйте протокол VTP.
    a) В качестве сервера VTP настройте SW1.
    b) Коммутаторы SW2 и SW3 настройте в качестве VTP клиента.
    c) Таблица VLAN должна содержать следующие сети:
        i) VLAN100 с именем **MGT**.
        ii) VLAN200 с именем **DATA**.
        iii) VLAN300 с именем **OFFICE**.
        iv) VLAN500 с именем **NATIVE**.
        v) VLAN600 с именем **SHUTDOWN**.
2) 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
3) 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.
4) Конфигурация протокола остовного дерева:
    a) Используйте протокол PVST.
    b) Коммутатор SW1 должен являться корнем связующего дерева в сетях VLAN 100, 200 и 300, в случае отказа SW1, корнем должен стать коммутатор SW2.
    c) Настройте порт F0/1 коммутатора SW1, таким образом, что при включении он сразу переходил в состояние forwarding не дожидаясь пересчета остовного дерева.

5) Настройте порты F0/10 коммутаторов SW2 и SW3 в соответствии с L2 диаграммой. Порты должны быть настроены в режиме доступа.
6) Между HQ1 и FW1 настройте взаимодействие по протоколу IEEE 802.1Q.
7) Отключите интерфейс F0/24 коммутатора SW1 и E5 межсетевого экрана FW1, которые использовались для первоначального конфигурирования сетевой инфраструктуры офиса HQ.
8) На всех устройствах, отключите неиспользуемые порты.
9) На всех коммутаторах, неиспользуемые порты переведите во VLAN 600.

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.
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 TFTP-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 PPPoE. Для этого настройте сервер PPPoE на BR1.
   c) Аутентификация PC2 на сервере PPPoE должна осуществляться по логину pc2user и паролю pc2pass.
   d) PC2 должен получать ip адрес от PPPoE сервера автоматически.

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 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.
5) 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

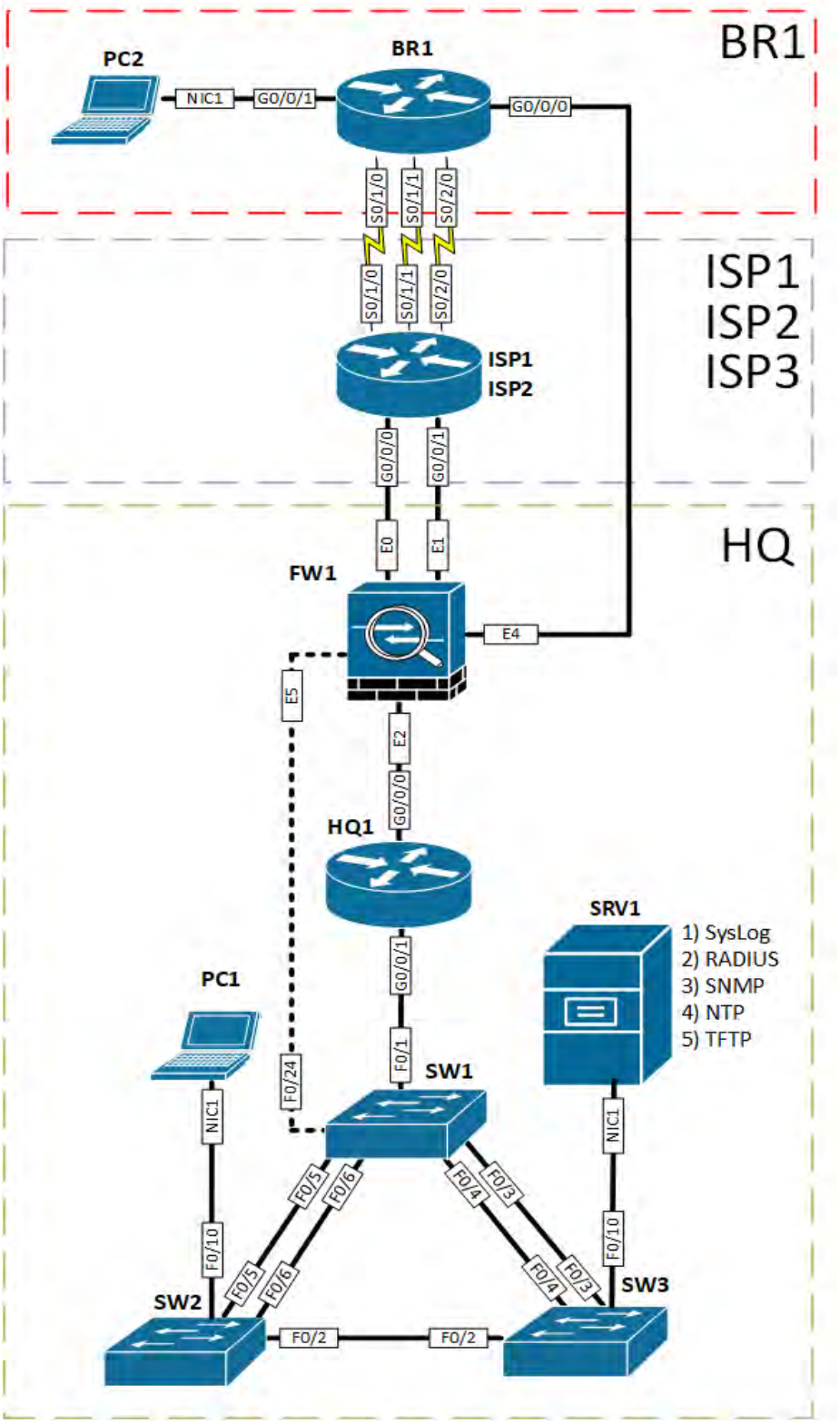
H. Конфигурация виртуальных частных сетей

1) Между HQ1 и BR1 настройте GRE туннель со следующими параметрами:

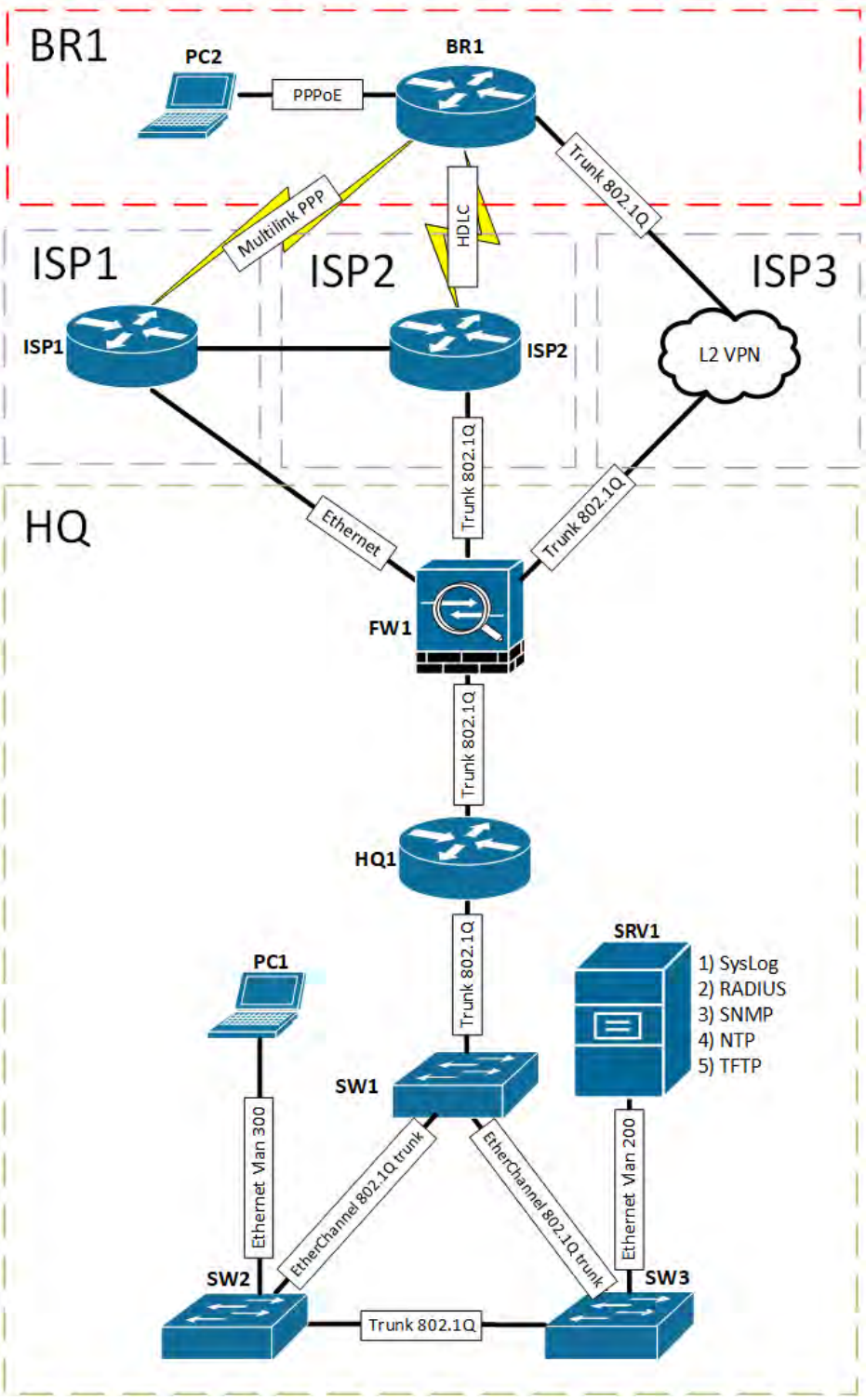
a) Используйте в качестве VTI интерфейс Tunnel1
b) Используйте адресацию в соответствии с L3-диаграммой
c) Режим — GRE
d) Интерфейс-источник — Loopback-интерфейс на каждом маршрутизаторе.
e) Обеспечьте работу туннеля с обеих сторон через провайдера ISP1

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.

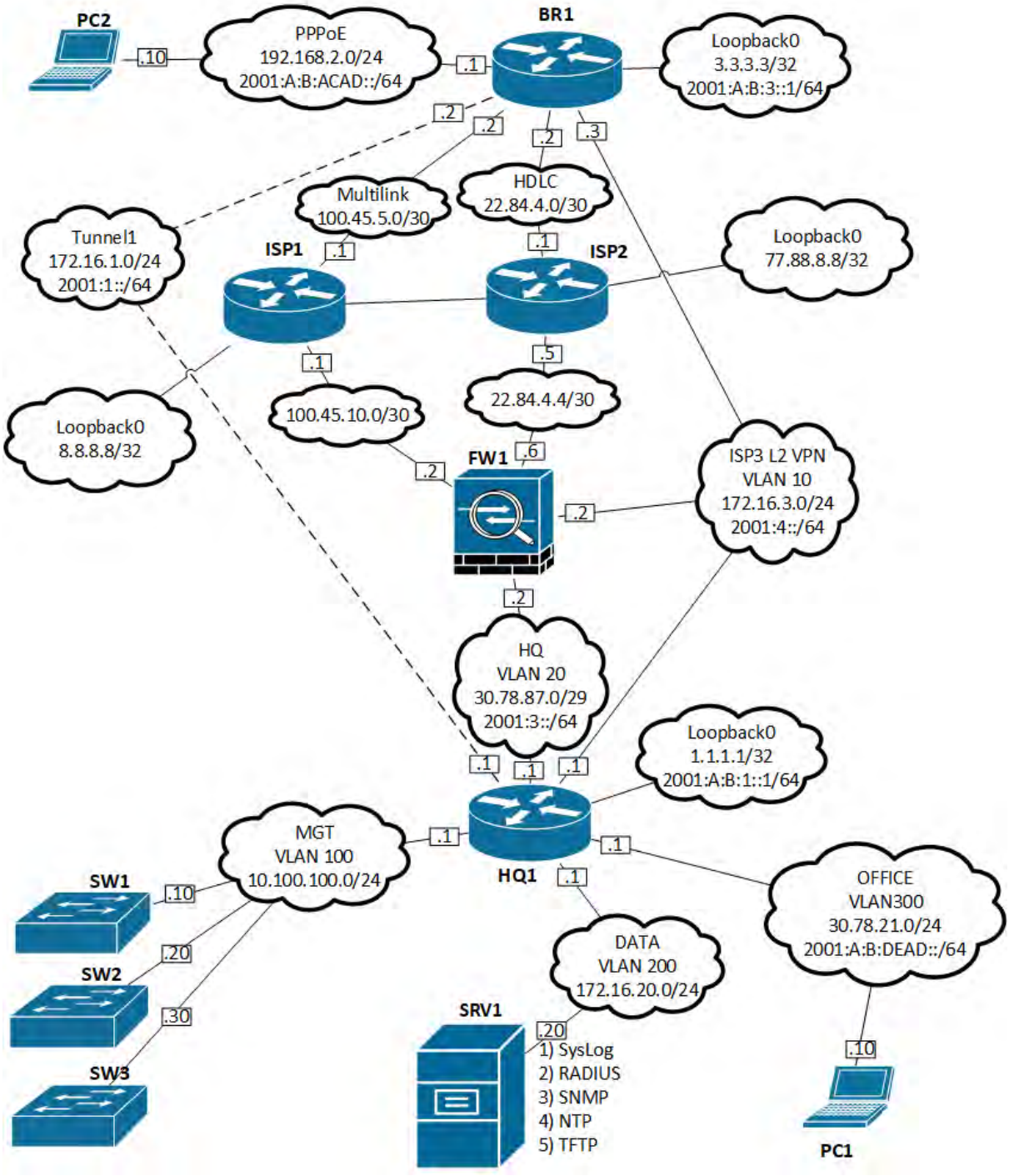
Топология L1


BR1
PC2
NIC1
G0/0/1
BR1
G0/0/0
S0/1/0
S0/1/1
S0/2/0
ISP1
ISP2
ISP3
S0/1/0
S0/1/1
S0/2/0
ISP1
ISP2
G0/0/0
G0/0/1
HQ
E0
E1
FW1
E4
E5
E2
G0/0/0
HQ1
SRV1
1) SysLog
2) RADIUS
3) SNMP
4) NTP
5) TFTP
G0/0/1
PC1
F0/1
SW1
F0/24
NIC1
NIC1
F0/5
F0/6
F0/4
F0/3
F0/10
F0/10
F0/5
F0/6
F0/4
F0/3
SW2
SW3
F0/2
F0/2

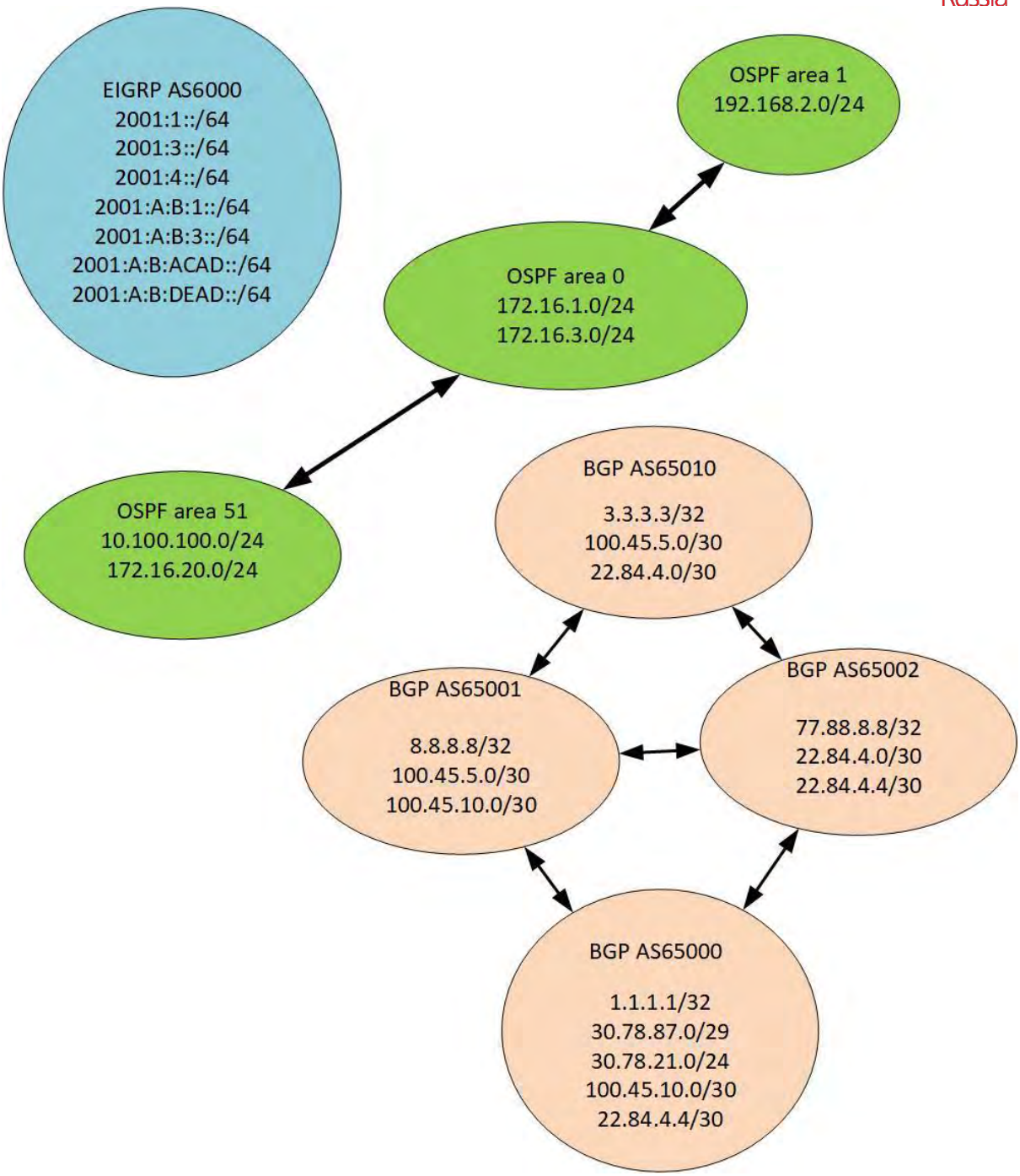
Топология L2



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
10.100.100.0/24
172.16.20.0/24
BGP AS65010
3.3.3.3/32
100.45.5.0/30
22.84.4.0/30
BGP AS65001
8.8.8.8/32
100.45.5.0/30
100.45.10.0/30
BGP AS65002
77.88.8.8/32
22.84.4.0/30
22.84.4.4/30
BGP AS65000
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

1) https://drive.google.com/file/d/17geWwpbCxa77cE2iQVFB1HKUti1KZx5a/view?usp=sharing
   Набор диаграмм Cisco
2) https://drive.google.com/file/d/1LW2QlWtVbwqfPieYUjCgpfzLaq1ZOYAs/view?usp=sharing
   Диаграмма сети Linux
3) https://drive.google.com/file/d/1Bn-RgYaahkDZY0AIsaYi00OYIYfbAWsS/view?usp=sharing
   Диаграмма сети Windows

Приложение 1

Дополнительные настройки модуля B

ВВЕДЕНИЕ

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

ОПИСАНИЕ ПРЕДУСТАНОВОК

Описание применяемых операционных систем

Имя компьютера	Операционная система
DC2	Windows Server 2019 GUI
CLI2	Windows 10 Enterprise
SRV2	Windows Server 2019 Core
R2	Windows Server 2019 GUI
DC1	Windows Server 2019 GUI
SRV1	Windows Server 2019 Core
R1	Windows Server 2019 Core
CLI1	Windows 10 Enterprise
DCA	Windows Server 2019 GUI

РЕКОМЕНДАЦИИ ПО ВЫДЕЛЕНИЮ ОПЕРАТИВНОЙ ПАМЯТИ ДЛЯ ВИРТУАЛЬНЫХ МАШИН

- Windows Server 2016 Core: минимум – 1 Gb, рекомендовано – 1,5 Gb;
- Windows Server 2016 GUI: минимум – 1,5 Gb, рекомендовано – 2 Gb;
- Windows 10 Enterprise: минимум – 1,5 Gb, рекомендовано – 2 Gb.

Приложение 2

Дополнительные настройки модуля C

ВВЕДЕНИЕ

Настоящие дополнения содержат конфигурационные файлы сетевых устройств.

ОПИСАНИЕ ПРЕДУСТАНОВОК

1. Данные конфигурационные файлы предназначены для подготовки стенда по Модулю C.

2. Перед использованием данных конфигурационных файлов, необходимо сбросить стартовую конфигурацию для всех устройств, а также удалить файл vlan.dat для коммутаторов.
3. Рекомендованные модели сетевых устройств:
   - HQ1, ISP, BR1 - Cisco 2900, 1940, 2800, 1840, 800 под управлением Cisco IOS Version 12.2 или выше.
   - SW1, SW2, SW3 - Cisco 2960 под управлением Cisco IOS Version 15.0 или выше.
   - FW1 - Cisco ASA5505, ASA5506 под управлением Cisco IOS Version 9.2 или выше.
4. В зависимости от используемой модели сетевого устройства, в конфигурационных файлах, необходимо отредактировать типы и номера интерфейсов.
5. Отредактировать диаграмму L1 под используемые модели сетевых устройств.

ПРЕДУСТАНОВКИ

```
###################### SW1 ######################
enable
conf t
!
enable password cisco
!
line vty 0 4
 password cisco
 transport input telnet
!
int vlan 1
 ip add 192.168.254.10 255.255.255.0
 no sh
!
end
wr

###################### SW2 ######################
enable
conf t
!
enable password cisco
!
line vty 0 4
 password cisco
 transport input telnet
!
int vlan 1
```

```
 ip add 192.168.254.20 255.255.255.0
 no sh
!
end
wr

###################### SW3 ######################
enable
conf t
!
enable password cisco
!
line vty 0 4
 password cisco
 transport input telnet
!
int vlan 1
 ip add 192.168.254.30 255.255.255.0
 no sh
!
end
wr



###################### HQ1 ######################
enable
conf t
!
enable password cisco
!
line vty 0 4
 password cisco
 transport input telnet
!
int F0/1
 no sh
 ip add 192.168.254.1 255.255.255.0
!
end
wr
```

```
###################### BR1 ######################
enable
conf t
!
enable password cisco
!
line vty 0 4
 password cisco
 transport input telnet
!
int f0/0
 no sh
 ip add 192.168.254.3 255.255.255.0
!
end
wr

###################### FW1 - ASA5505 ######################
enable

conf t
!
!
int E0/4
 no sh
!
int E0/5
 no sh
!
int vlan 1
 no sh
 nameif inside
 ip add 192.168.254.2 255.255.255.0
!
enable password cisco
!
username cisco password cisco
!
aaa authentication telnet console LOCAL
!
```

```
telnet 192.168.254.0 255.255.255.0 inside
!
end
wr

###################### FW1 - ASA5506 ######################

enable

conf t
!
!
int G1/4
 no sh
 nameif BR1
 security-level 100
 bridge-group 1
!
int G1/5
 no sh
 nameif HQ1
 security-level 100
 bridge-group 1
!
interface BVI 1
 nameif inside
 ip add 192.168.254.2 255.255.255.0
!
enable password cisco
!
username cisco password cisco
!
aaa authentication telnet console LOCAL
!
telnet 192.168.254.0 255.255.255.0 inside
telnet 192.168.254.0 255.255.255.0 BR1
telnet 192.168.254.0 255.255.255.0 HQ1
!
end
wr
```

```
###################### ISP ######################

en
conf t
!
no service password-encryption
!
hostname ISP
!
aaa new-model
!
aaa authentication ppp default local
aaa authentication login default local
aaa authorization network default local
!
no ip domain lookup
ip domain name worldskills.ru
!
username cisco priv 1 password 0 cisco
!
ip vrf ISP1
 rd 1:1
 route-target export 1:1
 route-target export 2:2
 route-target import 1:1
 route-target import 2:2
!
ip vrf ISP2
 rd 2:2
 route-target export 1:1
 route-target export 2:2
 route-target import 1:1
 route-target import 2:2
!
interface Multilink1
 ip vrf forwarding ISP1
 ip address 100.45.5.1 255.255.255.252
 peer default ip address pool PPP
 ppp multilink
 ppp multilink group 1
!
```

```
interface F0/0
 ip vrf forwarding ISP1
 no sh
 ip address 100.45.10.1 255.255.255.252
 desc to FW1 E0 from ISP1
 no shut
!
interface F0/1
 no shut
!
interface F0/1.901
 encapsulation dot1Q 901
 ip vrf forwarding ISP2
 ip address 22.84.4.5 255.255.255.252
 desc to FW1 E1 from ISP2
!
interface Serial0/1/0
 desc to BR1 from ISP1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
 clock rate 64000
 no shut
!
interface Serial0/2/0
 desc to BR1 from ISP1
 no ip address
 no shut
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
 clock rate 64000
!
interface Serial0/3/0
 ip vrf forwarding ISP2
 desc to BR1 from ISP2
 ip address 22.84.4.1 255.255.255.252
 no shut
 clock rate 64000
!
```

```
interface Loopback0
 ip vrf forwarding ISP1
 ip address 8.8.8.8 255.255.255.255
!
interface Loopback1
 ip vrf forwarding ISP2
 ip address 77.88.8.8 255.255.255.255
!
interface Loopback2
 ip address 11.11.11.11 255.255.255.255
!
interface Loopback3
 ip address 22.22.22.22 255.255.255.255
!
interface Tunnel1
 bandwidth 10000000
 ip vrf forwarding ISP1
 ip address 100.22.5.1 255.255.255.252
 no ip redirects
 ip mtu 9000
 tunnel source Loopback2
 tunnel destination 22.22.22.22
!
interface Tunnel2
 bandwidth 10000000
 ip vrf forwarding ISP2
 ip address 100.22.5.2 255.255.255.252
 no ip redirects
 ip mtu 9000
 tunnel source Loopback3
 tunnel destination 11.11.11.11
!
router bgp 65001
 bgp router-id 8.8.8.8
 bgp log-neighbor-changes
 neighbor 100.22.5.1 remote-as 65001
 !
 address-family ipv4
  no neighbor 100.22.5.1 activate
  no auto-summary
 exit-address-family
```

```
!
address-family ipv4 vrf ISP1
 bgp router-id 8.8.8.8
 redistribute static
 network 8.8.8.8 mask 255.255.255.255
 network 100.22.5.0 mask 255.255.255.252
 network 100.45.5.0 mask 255.255.255.252
 network 100.45.10.0 mask 255.255.255.252
 neighbor 100.22.5.2 remote-as 65001
 neighbor 100.22.5.2 activate
 neighbor 100.45.5.2 remote-as 65010
 neighbor 100.45.5.2 activate
 neighbor 100.45.5.2 default-originate
 neighbor 100.45.10.2 remote-as 65000
 neighbor 100.45.10.2 activate
 neighbor 100.45.10.2 default-originate
exit-address-family
!
address-family ipv4 vrf ISP2
 bgp router-id 77.88.8.8
 redistribute static
 network 77.88.8.8 mask 255.255.255.255
 network 100.22.5.0 mask 255.255.255.252
 network 22.84.4.0 mask 255.255.255.252
 network 22.84.4.4 mask 255.255.255.252
 neighbor 100.22.5.1 remote-as 65001
 neighbor 100.22.5.1 activate
 neighbor 22.84.4.2 remote-as 65010
 neighbor 22.84.4.2 local-as 65002 no-prepend replace-as
 neighbor 22.84.4.2 default-originate
 neighbor 22.84.4.2 activate
 neighbor 22.84.4.6 remote-as 65000
 neighbor 22.84.4.6 default-originate
 neighbor 22.84.4.6 local-as 65002 no-prepend replace-as
 neighbor 22.84.4.6 activate
exit-address-family
!
!
ip local pool PPP 100.45.5.2
ip forward-protocol nd
no ip http server
```

```
no ip http secure-server
!
ip route vrf ISP1 0.0.0.0 0.0.0.0 Null0
ip route vrf ISP2 0.0.0.0 0.0.0.0 Null0
!
line con 0
line aux 0
line vty 0 4
 transport input none
!
end
wr
```