**Конкурсное задание**

Компетенция

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 пуско-наладке 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 регионального чемпионат является утвержденным. В нем присутствуют 3 из 5 модулей, т.е. возможно набрать максимально 45 из 100 баллов

Конкурс включает в себя Пуско-наладку инфраструктуры на основе OC семейства Linux; Пуско-наладку инфраструктуры на основе OC семейства Windows; Пуско-наладку 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 по модульно, циклически по модулям А-B-C. Оценка каждого модуля происходит Ежедневно.

Задания разработаны и протестированы группой сертифицированных экспертов:

|  |  |  |
| --- | --- | --- |
| Модуль конкурсного задания | Роль | ФИО Эксперта |
| Модуль А: «Пуско-наладка инфраструктуры на основе OC семейства Linux» | Ведущий разработчик | М.М. Фучко |
| Модуль В: «Пуско-наладка инфраструктуры на основе OC семейства Windows» | Ведущий разработчик | А.Б. Мананников |
| Группа разработки | Д.В. Дюгуров |
| Модуль С: «Пуско-наладка телекоммуникационного оборудования» | Ведущий разработчик | Д.Н. Новиков |

## 3. МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ

Модули и время приведены в таблице 1

Таблица 1 – Время выполнение модуля

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование модуля | Рабочее время | Время на задание |
| 1 | Модуль А: «Пуско-наладка инфраструктуры на основе OC семейства Linux» | В соответствии с жеребьёвкой по циклу A-B-C | 5 ч. |
| 2 | Модуль В: «Пуско-наладка инфраструктуры на основе OC семейства Windows» | 5 ч. |
| 3 | Модуль С: «Пуско-наладка телекоммуникационного оборудования» | 5 ч. |

# Модуль А: «Пуско-наладка инфраструктуры на основе OC семейства Linux»

Версия 2019.1.0 от 28.02.19.

## ВВЕДЕНИЕ

Умение работать с системами на основе открытого исходного кода становится все более важным навыком для тех, кто желает построить успешную карьеру в ИТ. Данное 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 внутренней инфраструктуры ЦОД
* Конфигурация пограничной инфраструктуры ЦОД
* Конфигурация служб хранения данных ЦОД
* Конфигурация пользовательских служб ЦОД
* Конфигурация клиентских ВМ

## Секции независимы друг от друга, но вместе они образуют достаточно сложную инфраструктуру. Некоторые задания достаточно просты и понятны, некоторые могут быть не очевидными. Можно заметить, что некоторые технологии должны работать в связке или поверх других технологий. Например, динамическая маршрутизация должна выполнять поверх настроенного между организациями туннеля. Важно понимать, что если вам не удалось настроить полностью технологический стек, то это не означает, что работа не будет оценена. Например, для удаленного доступа необходимо сконфигурировать 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.

В случае недоступности DNS-сервисов сформируйте файл **/etc/hosts** в соответствии с **Таблицей 1** на всех хостах. Проверка по IP-адресам версии 4 выполняться не будет. В случае корректной работы DNS-сервисов изменения в файле **/etc/hosts** не требуются и могут повлечь потерю баллов за настройку DNS.

**Виртуальная машина ISP преднастроена и не требует доступа.**

**Доступ к остальным виртуальным машинам настроен по аккаунту root:toor**

**Доступ к клиентским виртуальным машинам настроен по аккаунту skill39:Skill39**

**Если при настройке служб у вас будет запрошен пароль, используйте Skill39**

## НЕОБХОДИМОЕ ОБОРУДОВАНИЕ, ПРИБОРЫ, ПО И МАТЕРИАЛЫ

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

Вам доступен диск debian-9.5.0-amd64-BD-1.iso

Вам доступен диск debian-9.5.0-amd64-BD-2.iso

**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, принимающими 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 **Топологией**.
2. Настройте IP-адресацию на ВСЕХ хостах в соответствии с **Таблицей 1**.
   1. Интерфейсы хостов в ЦОД(за исключением внешнего интерфейса FW) не должны иметь IPv4 адресов!
3. Установите дополнительные пакеты программного обеспечения:
   1. dnsutils
   2. lynx
   3. vim

## Конфигурация внутренней инфраструктуры ЦОД (Виртуальная машина CORE)

1. Реализуйте DNS-службу на основе пакета **BIND**:
   1. Сервер обслуживает зону **WSR.mv**
   2. Наполнение зоны организовать в соответствии с **Таблицей 2**
   3. Сервер реализует два отображения
      1. Внутреннее, для клиентов **CORE**, **STR**, **SRV-L**, **SRV-R**.
      2. Внешнее, для доступа **DNS-proxy** на **FW**
   4. Файлы зон расположить в **/var/dns**
   5. Сервер поддерживает прямое и обратное преобразование адресов для всех зон
2. Установите и настройте сервер каталогов LDAP на базе **OpenLDAP**:
   1. Создайте и распределите пользователей согласно **Таблице 4**
   2. Группы расположите в OU Groups
   3. Пользователей расположите в OU Users
      1. Пользователь сервиса VPN расположить в отдельном OU VPN
   4. Хосты **SRV-R. SRV-L**, **CORE** и и **STR** должны аутентифицироваться средствами LDAP
3. Установите и настройте службу синхронизации времени NTP на основе пакета **chrony**:
   1. Используется часовой пояс **MSK**(UTC+3)
   2. Время должно быть синхронизировано на всех хостах ЦОД
4. Реализуйте централизованный сбор и хранение сообщений журнала на основе пакета **Rsyslog**:
   1. Для хранения сообщений организовать файловую структуру в соответствии с **Таблицей 3**
   2. Все сообщения уровня **crit** и более критичных уровней дублировать в файл **/var/mylogs/CRIT.log**
5. Реализуйте центр сертификации на базе пакета **OpenSSL**
   1. В качестве базовой директории используйте /var/ca
   2. Атрибуты CA установите следующие:
      1. Страна RU
      2. Организация MV WSR
      3. CN CA установлен в MV WSR CA
   3. Создайте CA
   4. Все сертификаты должны быть выпущены данным СА
   5. Все компьютеры должны доверять данному СА.

## Конфигурация пограничной инфраструктуры ЦОД (Виртуальная машина FW)

1. Выполните конфигурацию сервера удаленного доступа **sshd**
   1. Прослушиваться должен только порт **1022**
   2. Запретите вход пользователю **root**
2. Реализуйте сервис удаленного доступа на основе технологии **OpenVPN**:
   1. В качестве сервера выступает **ВМ FW**
   2. Параметры туннеля
      1. Устройство TAP
      2. Порт сервера 1194
      3. Применяется сжатие трафика
      4. Адресацию выполнить в соответствии с **Таблицей 1.**
         1. Пользователь с сертификатом CN=Admin получет IP-адрес 10.9.9.77
      5. Используется TLS-аутентификация
   3. Все сертификаты должны быть выданы собственным **СА** на **ВМ CORE**
   4. Реализуйте дополнительную аутентификацию с помощью сервера OpenLDAP
      1. Разрешите доступ только пользователям из OU=VPN
   5. В качестве клиента выступают следующие ВМ
      1. **CLI-ADM**, cертификат CN=Admin
      2. **CLI-OUT**, сертификат CN=Guest
   6. OpenVPN-туннель должен предоставлять клиентам доступ к внутренним ресурсам сети организации
3. Реализуйте службу **DNS-Proxy** на базе пакета **BIND**
   1. Служба должна прослушивать внешний IPv4 адрес виртуальной машины **FW**
   2. Служба должна обращаться к основному **DNS-серверу** на **CORE**
   3. Служба должна разрешать запросы только от сервера **ISP.**
4. Настройте межсетевой экран **iptables**
   1. Входящие подключения должны быть разрешены к следующим службам
      1. **HTTP, HTTPS**, **DNS**, **OpenVPN**, **SSH**
   2. Если служба не настроена в соответствии с заданием — доступ должен быть запрещен

## Конфигурация служб хранения данных ЦОД (Виртуальная машина STR)

1. Настройте дисковый массив на основе технологии **RAID** на базе пакета **mdadm**
   1. Используйте два виртуальных диска
   2. Уровень массива RAID 1
   3. Используйте файловую систему ext4
   4. В качестве точки монтирования использовать **/mnt/storage**
   5. Массив должен автоматически монтироваться при запуске системы
2. Организуйте доступ к хранилищу данных с помощью технологии **NFS**
   1. Предоставьте доступ к каталогу **/mnt/storage**
   2. Доступ должен быть предоставлен на чтение и запись.
   3. Реализуйте объединение сетевых интерфейсов на **STR** и **CORE** по технологии **teaming** для достижения надежного канала и повышенной пропускной способности.

## Конфигурация пользовательских служб ЦОД

1. Реализуйте веб-службы на основе сервера **Apache**
   1. Раздается файл **/var/www/html/index.html**
   2. Файл должен содержать следующий текст
      1. «Served by <HOSTNAME>» где HOSTNAME — имя сервера
2. Реализуйте реверс-прокси сервер на базе пакета **nginx**
   1. Прослушивается внешний адрес FW
   2. Прослушиваются HTTP и HTTPS порты
      1. Выполняется перенаправление на HTTPS
   3. Запросы перенаправляются на сервера **SRV-R** и **SRV-L**
      1. Балансировка нагрузки осуществляется по принципу Round Robin
      2. Отключите кэширование ответов от серверов.

## Конфигурация клиентских ВМ

1. На ВМ CLI-ADM
   1. Настройте разрешение DNS-имен через сервер ISP
   2. Установите автоматическое подключение к OpenVPN -серверу на ВМ FW
      1. Используйте сертификат CN=Admin
      2. Подключение должно проходить по DNS-имени ВМ FW
      3. После подключения клиент должен перейти на использование сервера
      4. Выполнение авторизации должно быть автоматизировано
      5. Все конфигурационные файлы расположить в /etc/openvpn/
   3. Установить веб-браузер **IceWeasel\Firefox**
2. На ВМ CLI-OUT
   1. Настройте разрешение DNS-имен через сервер ISP
   2. Установите подключение к OpenVPN -серверу на ВМ FW
      1. Подключение должно включаться и отключаться по запуску скрипта
         1. **start\_vpn.sh** и **stop\_vpn.sh**
         2. Скрипт запрашивает учетные данные в ходе работы
      2. Используйте сертификат CN=GUEST
      3. Подключение должно проходить по DNS-имени ВМ FW
      4. После подключения клиент должен перейти на использование сервера
      5. Все конфигурационные файлы расположить в /etc/openvpn/
   3. Установить веб-браузер IceWeasel\Firefox

**Таблица 1** – Сетевая адресация

|  |  |  |
| --- | --- | --- |
| **Сеть** | **Хосты** | **Адреса/Подсети** |
| SRV | SRV-L | 2002:db:a::10 |
| SRV-R | 2002:db:a::20 |
| CORE | 2002:db:a::1 |
| STR | STR | 2002:db8:b::10 |
| CORE | 2002:db8:b::1 |
| INT | CORE | 2002:db8:c::10 |
| FW | 2002:db8:b::1 |
| EXT | FW | 10.10.10.10 |
| ISP | 10.10.10.1 |
| ADM | CLI-ADM | 20.20.20.10 |
| ISP | 20.20.20.1 |
| OUT | CLI-OUT | 30.30.30.10 |
| ISP | 30.30.30.1 |

**Таблица 2** – Учетные записи LDAP

|  |  |  |
| --- | --- | --- |
| **Хост** | **Внутреннее отображение** | **Внешнее отображение** |
| SRV-R | A: srv-r.wsr.mv  A: backend-l.wsr.mv CNAME: backend.wsr.mv |  |
| SRV-L | A: srv-r.wsr.mv  A: backend-r.wsr.mv CNAME: backend.wsr.mv |  |
| CORE | A: core.wsr.mv A: ns.wsr.mv |  |
| FW | A: fw.wsr.mv A: frontend.wsr.mv | A: fw.wsr.mv  CNAME: access.wsr.mv |
| STR | A: str.wsr.mv CNAME: storage.wsr.mv |  |

**Таблица 3** – Правила журналирования

|  |  |  |
| --- | --- | --- |
| **Источник** | **Уровень журнала** | **Файл** |
| SRV-R, SRV-L | WARN и выше | /var/mylogs/<HOSTNAME>/journal.log |
| STR | NOTICE и выше | /var/mylogs/<HOSTNAME>/journal.log |
| CORE | WARN и выше | /var/mylogs/<HOSTNAME>/journal.log |
| FW | WARN и выше | /var/mylogs/<HOSTNAME>/journal.log |

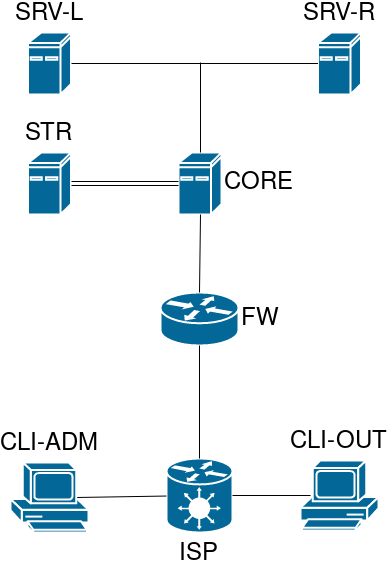
\*<HOSTNAME> - название директории для журналируемого хоста

\*\*В директории /var/mylogs/мне должно быть файлов, кроме тех, которые указаны в таблице

**Таблица 4** – Пользователи LDAP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Группа** | **OU** | **CN** | **Пароль** | **Доступ** |
| Administrators | Users | admin | toor | CORE, STR, SRV-L, SRV-R |
| Users | Users | user01-user10 | P@ssw0rd | SRV-L, SRV-R |
| VPN | VPN | vpn01-vpn02 | P@ssw0rd | OpenVPN на ВМ FW |

## ДИАГРАММА ВИРТУАЛЬНОЙ СЕТИ



# Модуль В: «Пуско-наладка инфраструктуры на основе OC семейства Windows»

Версия 1.0 от 15.02.2019.

## 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 Будапеште на восточном берегу Дуная. В главном офисе вы управляете доменом Pest.com. Вам необходимо настроить сервисы в локальной сети головного офиса.

Компания, в которой вы работаете, развивается и открывает еще один офис на западном берегу Дуная в районе старого города Буда. Вам придется настроить поддомен Buda.Pest.com.

Также Вам предстоит настроить канал связи между офисами с помощью интерфейсов вызовов по требованию.

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:
   1. данный файл с конкурсным заданием;
   2. файл дополнений к конкурсному заданию, содержащий: описание вида предустановок, описание используемых операционных систем, а также рекомендации по выделению ресурсов для виртуальных машин.
2. Предоставляемые конкурсантам компоненты проекта:
   1. файл для геренации пользователей в домене vuz (.txt);
   2. стартовая страница сайта it.vuz.ru (.htm);
   3. стартовая страница сайта www.vuz.ru (.htm);
   4. стартовая страница сайта filial.vuz.ru (.htm).
3. Программное обеспечение:
   1. Windows server 2016;
   2. Microsoft Office;
   3. RSAT tools for Windows 10;
   4. Windows 10 and Windows Server 2016 ADMX.

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

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

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

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

**Настройка DC1**

**Базовая настройка**

* переименуйте компьютер в DC1;
* задайте настройки сети в соответствии с таблицей 1;
* обеспечьте работоспособность брандмауэра и протокола ICMP (для использования команды ping).

**Active Directory**

* сделайте сервер основным контроллером домена vuz.ru.

**DHCP**

* настройте протокол DHCP для автоконфигурации клиентов;
* настройте failover: mode – Load balancer, partner server – FS1, state switсhover – 15 min, сообщения между серверами должны быть зашифрованы;
* область центрального офиса vuz.ru: диапазон выдаваемых адресов: 10.0.19.155-200/24;
* настройте дополнительные свойства области (адреса обоих DNS-серверов и основного шлюза).
* область филиала filial.vuz.ru: диапазон выдаваемых адресов: 10.0.20.155-200/24;

**DNS**

* настройте необходимые зоны прямого и обратного просмотра, обеспечьте их согласованную работу со службой DNS на FS1;
* создайте вручную все необходимые записи типа A и PTR для серверов домена и необходимых web-сервисов.

**GPO**

* запретите анимацию при первом входе пользователей в систему на всех клиентских компьютерах домена;
* члены группы IT должны быть членами группы локальных администраторов на всех клиентских компьютерах домена;
* в браузерах Internet Explorer и Edge должна быть настроена стартовая страница – https://www.vuz.ru;
* для членов группы Teachers настройте перенаправление папок My Documents и Desktop по адресу FS1→d:\shares\redirected;
* члены группы Teachers должны иметь повышенные требования к сложности пароля – не менее 12 символов.

**Элементы доменной инфраструктуры**

* создайте подразделения: IT, Teachers, Students, ITF;
* в соответствующих подразделениях создайте доменные группы: IT, Teachers, Students, ITF;
* также создайте доменную группу DAClients;

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

* создайте скрипт, при помощи которого сгенерируйте пользователей учебных групп (список групп в файле Groups.txt); поместите пользователей в соответствующие подразделения и группы, также поместите всех созданных пользователей в группу Students; все созданные учетные записи должны быть включены и доступны;
* если создать пользователей из файла не удается, создайте вручную по 1 пользователю в каждой группе с паролем P@ssw0rd;
* для каждого пользователя создайте домашнюю папку в папке по адресу FS1→d:\shares\users\Students, автоматически подключаемую в качестве диска Z:\;
* создайте пользователей adm и sup с паролем P@ssw0rd, поместите их в подразделение и группу IT;
* создайте пользователей adm1 и sup1 с паролем P@ssw0rd, поместите их в подразделение и группу ITF;
* создайте пользователей t1 и t2 с паролем P@ssw0rd, поместите их в подразделение и группу Teachers, для каждого пользователя создайте домашнюю папку в папке по адресу FS1→d:\shares\users\Teachers, автоматически подключаемую в качестве диска Z:\;

**Настройка FS1**

**Базовая настройка**

* переименуйте компьютер в FS1;
* задайте настройки сети в соответствии с таблицей 1;
* обеспечьте работоспособность брандмауэра и протокола ICMP (для использования команды ping);
* присоедините компьютер к домену vuz.ru;
* из трех имеющихся жестких дисков создайте RAID-5 массив; назначьте ему букву D:\.

**Active Directory**

* сделайте сервер дополнительным контроллером домена vuz.ru;
* контроллер не должен выполнять функцию глобального каталога;
* перенесите на него роль Infrastructure master.

**DHCP**

* настройте протокол DHCP для автоконфигурации клиентов;
* настройте failover: mode – Load balancer, partner server – DC, state switсhover – 15 min, сообщения между серверами должны быть зашифрованы;

**DNS**

* сделайте сервер дополнительным DNS-сервером в домене vuz.ru;
* загрузите c DC все зоны прямого и обратного просмотра.

**Общие папки**

* создайте общие папки (Students, Teachers) по адресу FS1→d:\shares\users, FS2→c:\shares\users; пользователи группы Teachers и IT должны иметь доступ на изменение пользовательских папок пользователей группы Students;
* создайте общую папку документов по адресу FS1→d:\shares\documents, FS2→c:\shares\ documents; создайте привязку для всех пользователей в качестве диска Y:;
* настройте разрешения папок в соответствии с таблицей 2;
* пользователи на любых сетевых дисках должны видеть только те папки, к которым им разрешен доступ.

**Квоты/Файловые экраны**

* установите максимальный размер в 50 Mb для каждой домашней папки пользователя группы Students (Z:\);
* запретите хранение в домашних папках пользователей файлов с расширениями .mp4, .avi, .vob; учтите, что файлы остальных типов пользователи вправе хранить в домашних папках.

**DFS**

* создайте корень под именем FILES, он должен поддерживаться FS1 и FS2;
* создайте под этим корнем папку с именем shares, ссылающуюся на сетевую директорию с тем же именем (shares), созданную Вами на диске D:;
* настройте репликацию между папками средствами DFS, исключите из репликации файлы с расширениями \*.avi.

**IIS**

* создайте сайт для учреждения www.vuz.ru (используйте предоставленный html-файл в качестве документа по умолчанию); сайт должен быть доступен только по протоколу https;
* создайте сайт для ИТ-службы учреждения it.vuz.ru (используйте предоставленный html-файл в качестве документа по умолчанию);
* сайт it.vuz.ru должен быть доступен только по протоколу https исключительно для членов группы IT по их пользовательским сертификатам.

**Настройка RCA**

**Базовая настройка**

* переименуйте компьютер в RCA;
* задайте настройки сети в соответствии с таблицей 1;
* обеспечьте работоспособность брандмауэра и протокола ICMP (для использования команды ping);
* присоедините компьютер к домену vuz.ru.

**Службы сертификации**

* установите службы сертификации;
* настройте одиночный корневой сервер сертификации (длина ключа и алгоритмы шифрования значения не имеют);
* имя центра сертификации – VuzRootCA;
* срок действия сертификата – 15 лет.
* настройте шаблон выдаваемого сертификата для клиентских компьютеров *VuzClients*: *subject name=common name*, автозапрос для всех клиентских компьютеров домена;
* настройте шаблон выдаваемого сертификата для группы IT *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);
* присоедините компьютер к домену Pest.com;
* установите набор компонентов удаленного администрирования RSAT;
* запретите использование «спящего режима» таким образом, чтобы пользователи домена не могли изменить эту настройку без участия администратора домена;
* используйте компьютер для тестирования настроек в домене Pest.com: пользователей, общих папок, групповых политик, в том числе – тестирования удаленных подключений через Direct Access (временно переключая компьютер в сеть Internet).

**Настройка BR1**

**Базовая настройка**

* переименуйте компьютер в BR1;
* задайте настройки сети в соответствии с таблицей 1;
* обеспечьте работоспособность брандмауэра и протокола ICMP (для использования команды ping);
* присоедините компьютер к домену vuz.ru.

**Настройка RRAS**

* установите службу RRAS;
* настройте проброс запросов и ответов DHCP из филиала в центральный офис;
* настройте защищенное соединение Site-to-Site VPN с удаленным филиалом, весь трафик между доменами должен передаваться через это соединение, сертификаты должны быть выданы RCA;

**Работа с DC2**

**AD**

* сделайте сервер дополнительным контроллером домена vuz.ru в режиме RODC;
* разрешите локальную авторизацию пользователей группы ITF.

**WDS**

* разверните роль WDS, она должна отвечать на запросы любых клиентских компьютеров;
* для локального хранения образов используйте папку E:\RemoteInstall, для этого используйте дополнительный жесткий диск (при необходимости измените инфраструктуру виртуальной машины);
* подготовьте для развертывания Windows 10 Enterprise, образ которой Вам доступен;
* членам группы IT предоставьте полный доступ к распространяемому образу ОС;
* установите на компьютер CLI2 операционную систему с помощью настроенной службы развертывания.

**Работа с RDS**

**Службы удаленных рабочих столов**

* разверните терминальный сервер, не устанавливайте и не настраивайте компоненты лицензирования.
* сконфигурируйте web-доступ RemoteApp к службам терминалов сервера;
* опубликуйте программу *Notepad* на web-портале RemoteApp для членов группы IT;
* опубликуйте программу *Paint* на web-портале RemoteApp для членов группы Students;
* web-интерфейс сервера должен быть настроен таким образом, чтобы пользователи могли автоматически получать доступ к форме входа на web-интерфейс удаленных рабочих столов при указании адресов http://rds.vuz.ru и https://rds.vuz.ru;
* c помощью доменного центра сертификации на сервере RCA сгенерируйте и используйте для терминальных служб соответствующий SSL-сертификат. Сертификат должен быть использован для всех установленных компонентов терминальных служб. При обращении с любого компьютера в домене vuz.ru к сайту по имени https://rds.vuz.ru сертификат должен распознаваться как доверенный и действительный.

**Работа с FS2**

**Квоты/Файловые экраны**

* установите максимальный размер в 50 Mb для каждой домашней папки пользователя группы Students (Z:\);
* запретите хранение в домашних папках пользователей файлов с расширениями .mp4, .avi, .vob; учтите, что файлы остальных типов пользователи вправе хранить в домашних папках.

**DFS**

* создайте корень под именем FILES, он должен поддерживаться FS1 и FS2;
* создайте под этим корнем папку с именем shares, ссылающуюся на сетевую директорию с тем же именем (shares), созданную Вами на диске D:;
* настройте репликацию между папками средствами DFS, исключите из репликации файлы с расширениями \*.avi.

**IIS**

* создайте сайт filial.vuz.ru (используйте предоставленный htm-файл в качестве документа по умолчанию);
* сайт должен быть доступен только по протоколу https с использованием сертификата, выданного RCA.

**Работа с CLI2**

**Базовая настройка**

* установите операционную систему с помощью службы развертывания;
* дайте имя компьютеру CLI2;
* IP-адрес должен назначаться сервером DHCP центрального офиса;
* обеспечьте работоспособность брандмауэра и протокола ICMP (для использования команды ping);
* присоедините компьютер к домену vuz.ru;
* запретите использование «спящего режима»;
* используйте компьютер для тестирования настроек.

**Настройка BR2**

**Базовая настройка**

* переименуйте компьютер в BR2;
* задайте настройки сети в соответствии с таблицей 1;
* обеспечьте работоспособность брандмауэра и протокола ICMP (для использования команды ping);
* присоедините компьютер к домену vuz.ru.

**Настройка RRAS**

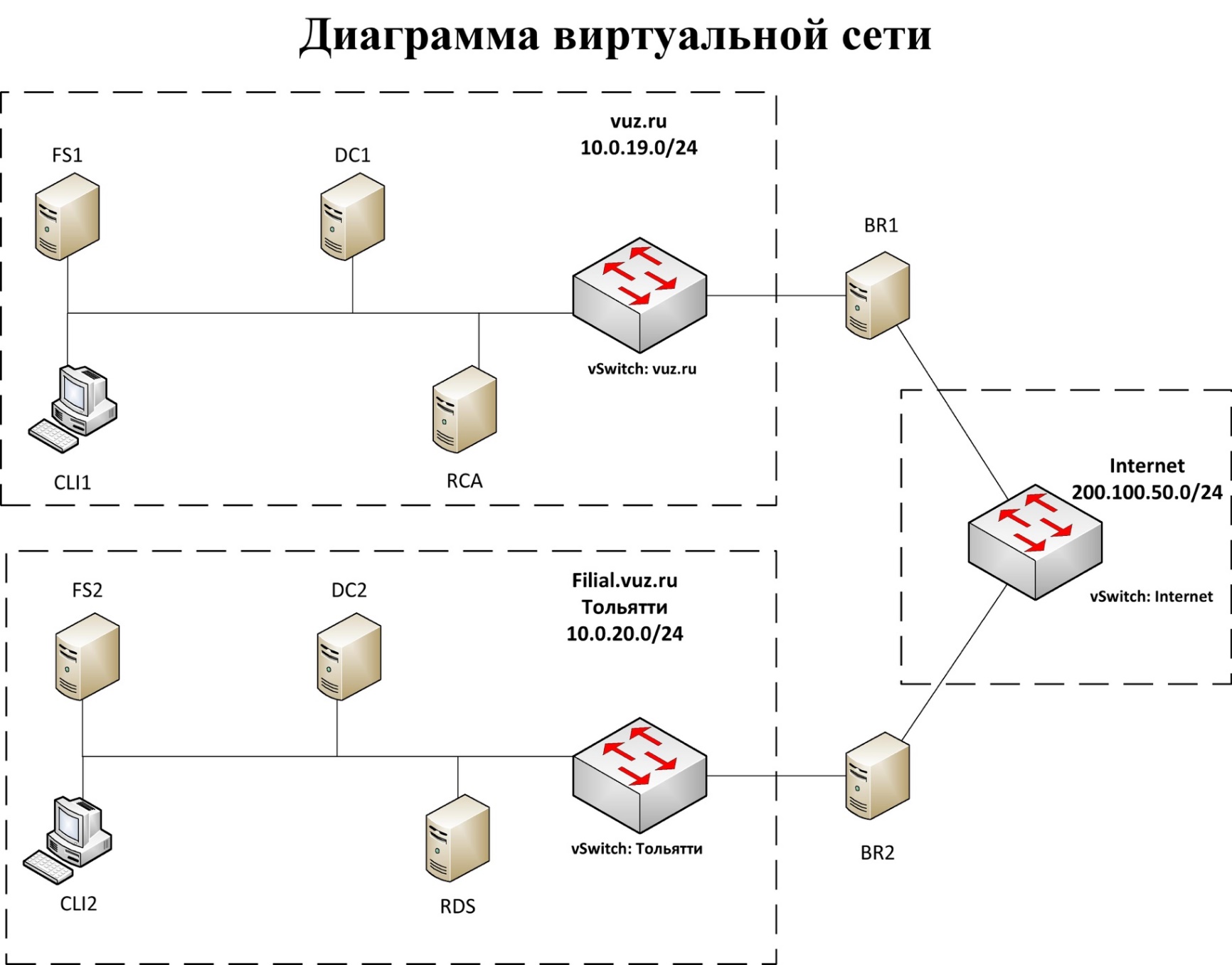
* установите службу RRAS;
* настройте проброс запросов и ответов DHCP из удаленного офиса в центральный;
* настройте защищенное соединение Site-to-Site VPN с центральным офисом, весь трафик между офисами должен передаваться через это соединение, сертификаты должны быть выданы RCA;
* настройте проброс портов для доступа удаленных клиентов (проверяется из сети Internet) к сайтам www.vuz.ru и filial.vuz.ru.

**Таблица 1** – Адресация сети

|  |  |
| --- | --- |
| **Имя компьютера** | **IP-адреса** |
| DC1 | 10.0.19.1/24 |
| FS1 | 10.0.19.2/24 |
| RCA | 10.0.19.3/24 |
| BR1 | 10.0.19.254/24  200.100.50.100/24 |
| CLI1 | DHCP |
| DC2 | 10.0.20.1/24 |
| FS2 | 10.0.20.2/24 |
| RDS | 10.0.20.3/24 |
| BR2 | 10.0.20.254/24  200.100.50.101/24 |
| CLI2 | DHCP |
| INET | 200.100.50.200/24 |

**Таблица 2** – Файловые ресурсы

|  |  |  |  |
| --- | --- | --- | --- |
| **Имя общего ресурса** | **Расположение** | **Доступ только для чтения** | **Доступ для чтения и записи** |
| Documents | FS1→D:\shares\documents  FS2→C:\shares\documents | Students | Teachers  IT |
| Teachers | FS1→D:\shares\users\teachers  FS2→C:\shares\users\teachers | - | Teachers  IT |
| Students | FS1→D:\shares\users\students  FS2→C:\shares\users\students | Teachers | Students  IT |



# Модуль С: «Пуско-наладка телекоммуникационного оборудования»

Версия: 1.0 от 28.02.19.

## 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 FrameRelay 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.

Следует обратить внимание, что задание составлено не в хронологическом порядке. Некоторые секции могут потребовать действий из других секций, которые изложены ниже. 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 консольное подключение.

## Базовая настройка

1. Задайте имена ВСЕХ устройств в соответствии с топологией
2. Назначьте для ВСЕХ устройств доменное имя **wsrvuz19.ru**
3. Создайте на ВСЕХ устройствах пользователя **wsrvuz19** с паролем **cisco**
   1. Пароль пользователя должен храниться в конфигурации в виде результата хэш-функции.
   2. Пользователь должен обладать максимальным уровнем привилегий.
4. Для ВСЕХ устройств реализуйте модель AAA.
   1. Аутентификация на удаленной консоли должна производиться с использованием локальной базы данных (кроме устройства RTR1 и RTR2)
   2. После успешной аутентификации при входе с удаленной консоли пользователь сразу должен попадать в режим с максимальным уровнем привилегий.
   3. Настройте необходимость аутентификации на локальной консоли.
   4. При успешной аутентификации на локальной консоли пользователь должен попадать в режим с минимальным уровнем привилегий.
   5. На BR3 при успешной аутентификации на локальной консоли пользователь должен попадать в режим с максимальным уровнем привилегий
5. На ВСЕХ устройствах установите пароль **wsr** на вход в привилегированный режим.
   1. Пароль должен храниться в конфигурации НЕ в виде результата хэш-функции.
   2. Настройте режим, при котором все пароли в конфигурации хранятся в зашифрованном виде.
6. На маршрутизаторе RTR1 на виртуальных терминальных линиях с 0 по 15 настройте аутентификацию с использованием RADIUS-сервера.
   1. Порядок аутентификации:
      1. По протоколу RADIUS
      2. Локальная
   2. Используйте общий ключ **cisco**
   3. Используйте номера портов 1812 и 1813 для аутентификации и учета соответственно
   4. Адрес RADIUS-сервера **2001::300:2**
   5. Настройте авторизацию при успешной аутентификации
   6. Проверьте аутентификацию по протоколу RADIUS при удаленном подключении к маршрутизатору RTR1, используя учетную запись **radius** с паролем **cisco**
   7. Включите блокировку на 1 минуту в случае неправильного ввода пароля в течение 30 секунд
7. На ВСЕХ устройствах создайте виртуальные интерфейсы, подынтерфейсы и интерфейсы типа петля. Назначьте IP-адреса в соответствии с топологией
   1. Включите механизм SLAAC для выдачи IPv6-адресов в сети MNG на интерфейсе маршрутизатора RTR1
   2. На виртуальных интерфейсах в ВЛВС 100 (MNG) на коммутаторах SW1, SW2, SW3 включите режим автоконфигурации IPv6
   3. На коммутаторах SW1,SW2,SW3 присвойте соответственно link-local IPv6-адреса fe80::10, fe80::20 и fe80::30 в ВЛВС MNG
   4. На ВСЕХ коммутаторах отключите ВСЕ неиспользуемые порты и переведите в VLAN 99.
8. Все устройства должны быть доступны для управления по протоколу SSH версии 2.
9. На маршрутизаторе RTR1 установите правильное время с учётом часового пояса.

## Настройка коммутации

1. На ВСЕХ коммутаторах создайте ВЛВС:
   1. под номером 99 с именем UNUSED
   2. под номером 100 с именем MNG
   3. под номером 300 с именем OFFICE
2. На коммутаторах SW1, SW2 и SW3 выполните настройку протокола динамического согласования транков (DTP).
   1. На коммутаторе SW3 переведите порты в Fa0/3-6 в режим, при котором коммутатор на данных портах будет инициировать согласование параметров транка.
   2. Переведите порты Fa0/3-4 на SW1 и Fa0/5-6 на SW2 в режим, при котором каждый коммутатор ожидает начала согласования параметров от соседа, но сам не инициирует согласование.
   3. Переведите порты Fa0/1-2 на SW1 и SW2 в режим передачи трафика по протоколу IEEE 802.1q. Явно отключите динамическое согласование транков.
3. Настройте агрегирование каналов связи между коммутаторами.
   1. Номера портовых групп:
      1. 1 — между коммутаторами SW1 <-> SW2;
      2. 2 — между коммутаторами SW2 <-> SW3;
      3. 3 — между коммутаторами SW3 <-> SW1.
   2. Коммутатор SW3 должен быть настроен в режиме пассивного согласования по обеим портовым группам по протоколу PAgP;
   3. Коммутаторы SW1 и SW2 должны быть настроены в активном режиме PAgP с коммутатором SW3.
   4. Коммутатор SW2 должен быть настроен в режиме активного согласования по протоколу LACP с коммутатором SW1.
   5. Коммутатор SW1 должен быть настроен в режиме пассивного согласования по протоколу LACP с коммутатором SW2.
4. Конфигурация протокола остовного дерева:
   1. Используйте протокол Rapid STP.
   2. Коммутатор SW1 должен являться корнем связующего дерева в VLAN 100,300. В случае его отказа, корнем должен стать коммутатор SW2.
5. На портах Fa0/5, Fa0/9 коммутатора SW1 включите защиту от нежелательных BPDU. При получении BPDU на этом порту, порт должен переводиться в состояние err-disabled.
6. Обеспечить автоматическое восстановление работоспособности указанных портов с интервалом 60 секунд
7. Настройте порты Fa0/5, Fa0/9 коммутатора SW1 таким образом, чтобы порт переходил в состояние Forwarding, не дожидаясь пересчета остовного дерева.

## Настройка подключений к глобальным сетям

1. Настройте подключение PPPoE между RTR1 и маршрутизатором BR1.
   1. Настройте PPPoE клиент на BR1.
   2. Используйте имя пользователя **cisco** и пароль **cisco**
   3. Устройства походят одностороннюю аутентификацию по протоколу CHAP, только RTR1 проверяет имя пользователя и пароль.
   4. BR1 должен автоматически получать адрес от RTR1.
2. Настройте подключение RTR1 к провайдеру ISP с помощью протокола PPP.
   1. Настройте Multilink PPP с использованием двух Serial-интерфейсов.
   2. Используйте 1 номер интерфейса.
   3. Не используйте аутентификацию.
3. RTR1 должен автоматически получать адрес от ISP.

## Настройка маршрутизации

1. На маршрутизаторах ISP, RTR1 и BR1 настройте протокол динамической маршрутизации OSPFv3 с номером процесса 1.
   1. Включите маршрутизацию для сетей BR1, OFFICE, Tunnel100, Tunnel101 а также на интерфейсе Loopback100 маршрутизатора RTR1 и на интерфейсе Loopback101 маршрутизатора BR1.
   2. Используйте области согласно диаграмме маршрутизации
   3. Настройте суммаризацию для сетей на интерфейсах Loopback101 и сети BR1 маршрутизатора BR1 таким образом, чтобы BR1 анонсировал вместо этих двух сетей только одну суммарную сеть минимально возможного размера. Используйте для этих интерфейсов область 1.
   4. Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.
2. На маршрутизаторах ISP, RTR2 и BR1 настройте протокол динамической маршрутизации OSPF с номером процесса 1.
   1. Включите маршрутизацию для сетей BR1, OFFICE, Tunnel100, Tunnel101 а также на интерфейсе Loopback100 маршрутизатора RTR1 и на интерфейсе Loopback101 маршрутизатора BR1.
   2. Используйте алгоритм аутентификации md5 с ключом WSR.
   3. Используйте области согласно диаграмме маршрутизации
   4. Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.
3. На маршрутизаторах RTR1 и BR1 настройте протокол динамической маршрутизации EIGRP с номером автономной системы 2019.
   1. Включите в обновления маршрутизации сети Tunnel100, Loopback100 и Loopback101,
   2. Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.

## Настройка служб

1. В сетевой инфраструктуре сервером синхронизации времени является RTR2. Все остальные сетевые устройства должны использовать в качестве сервера времени RTR1.
   1. Передача данных между RTR1 и RTR2 осуществляется без аутентификации.
   2. Настройте временную зону с названием EKB, укажите разницу с **UTC +5** часов.
   3. Настройте сервер синхронизации времени. Используйте стратум **2**.
   4. Используйте для синхронизации клиентов с RTR1 аутентификацию MD5 с ключом **WSR**.
2. Настройте на RTR1 DHCPv6 сервер с отслеживанием состояния для сети OFFICE со следующими характеристиками:
   1. Имя домена **wsrvuz19.ru**
   2. DNS – сервер – адрес ISP
3. Обеспечить копирование с коммутатора SW1 на BR1 файла SW1\_backup, являющийся копией стартовой конфигурации SW1
4. **!!! ДАННЫЙ ПУНКТ ОЦЕНИВАЕТСЯ В СОСТАВЕ МОДУЛЯ A (LINUX) !!!**

На маршрутизаторе RTR2 настройте RADIUS – сервер (программное обеспечение предустановлено):

* 1. Используйте общий ключ **cisco**
  2. Используйте номера портов 1812 и 1813 для аутентификации и учета соответственно
  3. Адрес сети **2001::300:0/64**
  4. Учетная запись **radius** с паролем **cisco**

***Настройка механизмов отказоустойчивости***

1. На шлюзе RTR1 и узле RTR2 настроить протокол VRRP в сети OFFICE:
   1. Номер группы 300
   2. IP адрес виртуального шлюза 172.16.0.1/24
   3. Master – RTR1
   4. Backup – RTR2

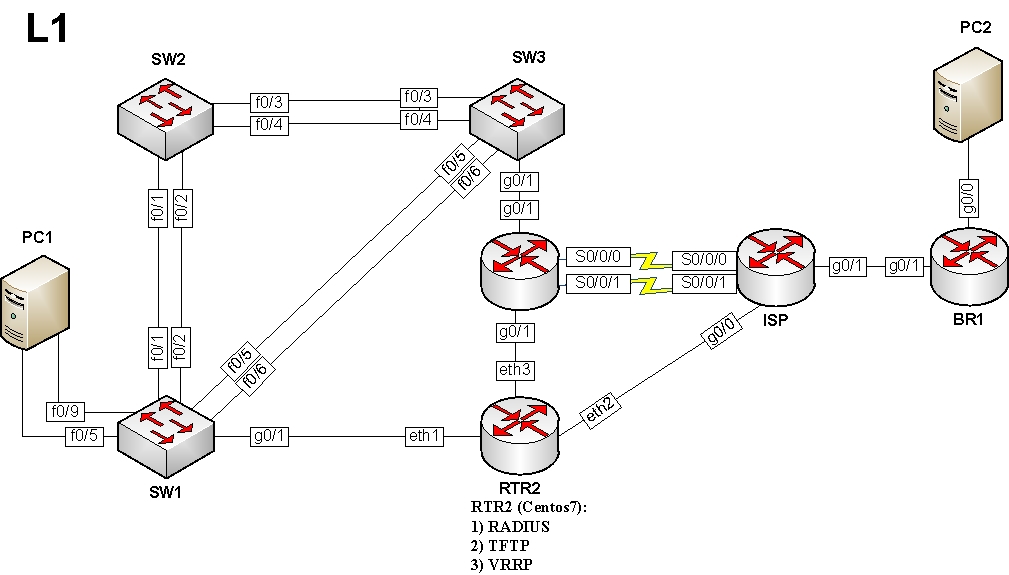
## Настройка механизмов безопасности

1. На порту коммутатора SW1, к которому подключен PC1, включите и настройте Port Security со следующими параметрами:
   1. не более 3 адресов на интерфейсе
   2. адреса должны динамически пополняться и сохраняться в текущей конфигурации
   3. при попытке подключения устройства с адресом, нарушающим политику, порт не должен быть отключен, уведомления не передаются
2. На маршрутизаторе RTR настройте на интерфейсе, ведущем в сторону провайдера ISP, список контроля доступа со следующими свойствами:
   1. ACL должен позволять пользователям сети OFFICE выходить во внешнюю сеть
   2. ACL не должен нарушать работу настроенных сервисов и протоколов
   3. ACL должен позволять отправлять эхо-запросы из внутренней сети и получать на них ответы.

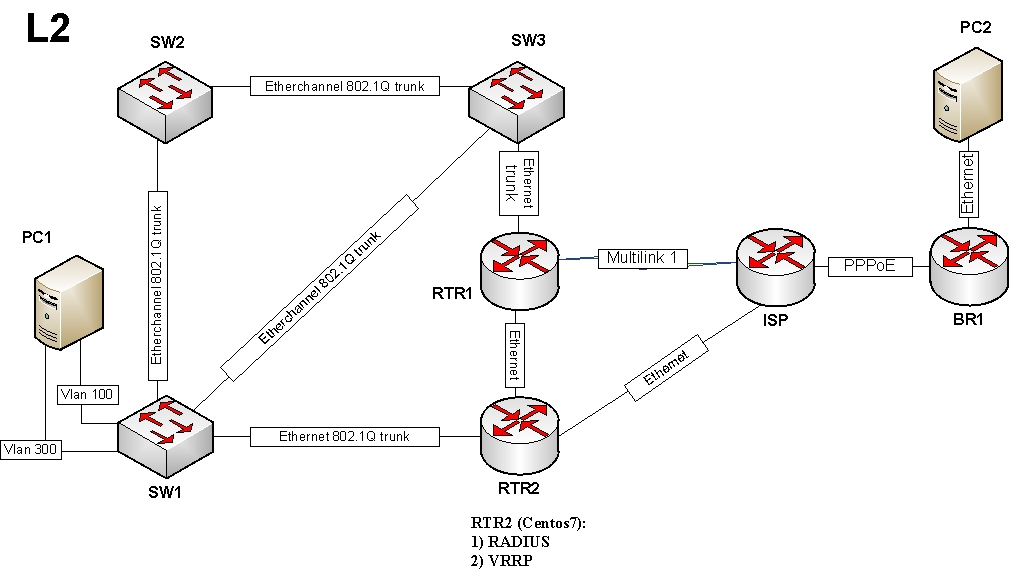
## Конфигурация виртуальных частных сетей

1. На маршрутизаторах RTR1 и BR1 настройте GRE-туннель:
   1. Используйте в качестве VTI интерфейс Tunnel100
   2. Используйте адресацию согласно диаграмме.
2. На маршрутизаторах RTR1 и BR1 настройте IKEv1 IPsec Site-to-Site VPN и примените его к созданному GRE-туннелю
   1. Параметры политики первой фазы:
      1. Проверка целостности – MD5
      2. Шифрование – DES
      3. Группа Диффи-Хэлмана – 14
      4. Ключ - cisco
   2. Параметры преобразования трафика для второй фазы:
      1. Протокол – ESP
      2. Шифрование – DES
      3. Проверка целостности – MD5
3. На маршрутизаторах RTR2 и BR1 настройте GRE-туннель:
   1. Используйте в качестве VTI интерфейс Tunnel101
   2. Используйте адресацию согласно диаграмме.

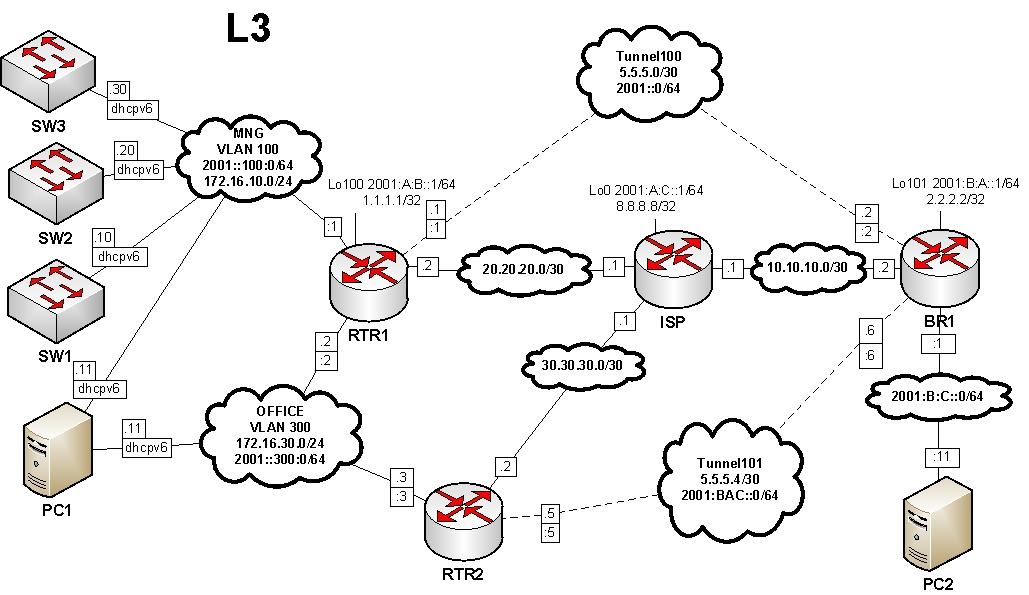
## Топология L1



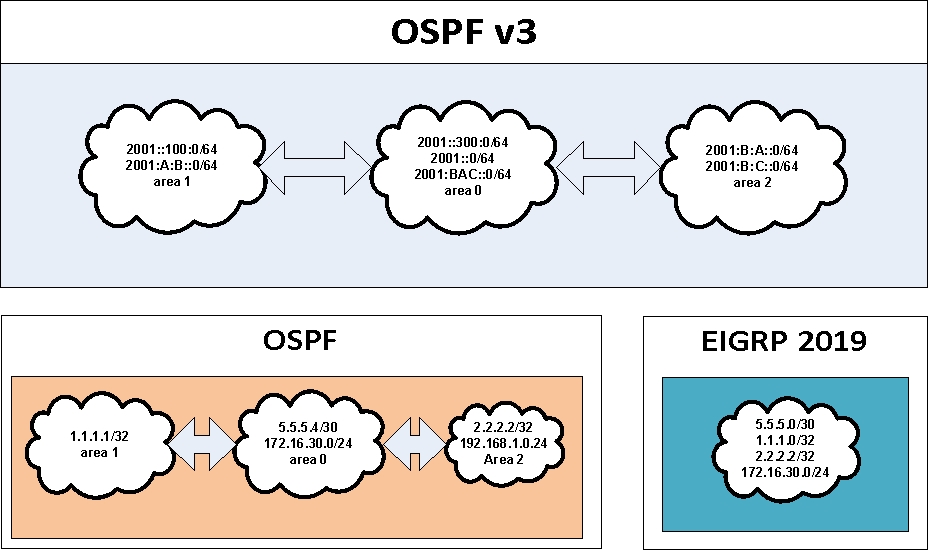
## Топология L2



## Топология L3



## Routing-диаграмма



## 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 |
| А | Модуль А: «Пуско-наладка инфраструктуры на основе OC семейства Linux» | 0 | 15 | 15 |
| В | Модуль В: «Пуско-наладка инфраструктуры на основе OC семейства Windows» | 0 | 15 | 15 |
| С | Модуль С: «Пуско-наладка телекоммуникационного оборудования» | 0 | 15 | 15 |
| Итого = | | 0 | 45 | 45 |

**Субъективные оценки -** Не применимо.

**5. Приложения к заданию**