**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: 6 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 24 из 100 баллов

Конкурс включает в себя “Пусконаладку инфраструктуры на основе OC семейства Linux”; “Пусконаладку инфраструктуры на основе OC 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.

Задания разработаны и протестированы группой сертифицированных экспертов:

3. МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ

Модули и время приведены в таблице 2.

 **Таблица 2 –** Время выполнение модуля

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

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

Версия 1 от 31.08.19.

## 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 сетевой инфраструктуры
* Службы централизованного управления и журналирования
* Конфигурация служб удаленного доступа
* Конфигурация веб-служб
* Конфигурация служб хранения данных
* Конфигурация параметров безопасности

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-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 используется **CentOS**

Вам доступен диск CentOS-7-x86\_64-Everything-1810.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:
3. tcpdump
4. net-tools
5. curl
6. vim
7. lynx
8. dhclient
9. bind-utils
10. nfs-utils
11. cifs-utils
12. 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.
13. В случае корректной работы DNS-сервисов ответы DNS должны иметь более высокий приоритет.

**Конфигурация сетевой инфраструктуры**

1. Настройте IP-адресацию на ВСЕХ хостах в соответствии с **Диаграммой**.
2. Настройте сервер протокола динамической конфигурации хостов для L-CLI
	1. В качестве DHCP-сервера используйте L-FW
		1. Используйте пул адресов 172.16.100.65 — 172.16.100.75 для сети L-CLI
		2. Используете адрес L-SRV в качестве адреса DNS-сервера.
	2. Настройте DHCP-сервер таким образом, чтобы L-CLI всегда получал фиксированный IP-адрес в соответствии с **диаграммой.**
	3. В качестве шлюза по умолчанию используйте адрес соответствующего интерфейса L-FW.
	4. Используйте DNS-суффикс **skill39.wsr.**
	5. DNS-записи типа A и PTR хостов должны обновляться при получении им адреса от DHCP-сервера.
3. На L-SRV настройте службу разрешения доменных имен
	1. Сервер должен обслуживать зону **skill39.wsr.**
	2. Сопоставление имен организовать в соответствии с **Таблицей 1.**
	3. Запросы, которые выходят за рамки зоны **skill39.wsr** должны пересылаться DNS-серверу ISP. Для проверки используйте доменное имя **ya.ru**.
	4. Реализуйте поддержку разрешения обратной зоны.
	5. Файлы зон располагать в **/opt/dns/**
4. На L-FW настройте интернет-шлюз для организации коллективного доступа в Интернет.
	1. Настройте трансляцию сетевых адресов из внутренней сети в адрес внешнего интерфейса.
	2. Организуйте доступность сервиса DNS на L-SRV по внешнему адресу L-FW.
		1. Сервер L-FW должен перенаправлять внешние DNS запросы из сети Интернет на L-SRV. Важно преобразовывать только [www.skill39.wsr](http://www.skill39.wsr/) во внешний адрес L-FW.

**Службы централизованного управления и журналирования**

1. На L-SRV организуйте централизованный сбор журналов с хостов L-FW, L-SRV.
	1. Журналы должны храниться в директории **/opt/logs/.**
	2. Журналирование должно производится в соответствии с **Таблицей 2.**

**Конфигурация служб удаленного доступа**

1. На L-FW настройте удаленный доступ по протоколу SSH:
	1. Доступ ограничен пользователями **ssh\_p, root** и **ssh\_c**
		1. В качестве пароля пользователь (кроме root) использовать **ssh\_pass.**
		2. root использует стандартный пароль
	2. SSH-сервер должен работать на порту **22**
2. На L-CLI настройте клиент удаленного доступа SSH:
	1. 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 L-SRV установите и настройте веб-сервер apache:
	1. Настройте веб-сайт для внешнего пользования www.skill39.wsr.
		1. Используйте директорию **/var/www/html/out.**
		2. Используйте порт 8088.
		3. Сайт предоставляет доступ к двум файлам.
			1. index.html, содержимое “Hello, [www.skill39.wsr](http://www.skill39.wsr) is here!”
			2. date.php(исполняемый PHP-скрипт), содержимое:
				1. Вызов функции date('Y-m-d H:i:s');
2. На L-FW настройте реверс-прокси на основе NGINX:
	1. Сайт www.skill39.wsr должен быть доступен из внешней сети по внешнему адресу L-FW
	2. Все настройки, связанные с заданием, должны содержаться в отдельном конфигурационном файле в каталоге /etc/nginx/conf.d/task.conf
		1. Конфигурация основного файла должна быть минимальной и не влиять на работу NGINX в рамках выполнения задания.

**Конфигурация служб хранения данных**

1. Реализуйте синхронизацию каталогов на основе демона rsyncd.
	1. В качестве сервера синхронизации используется L-SRV.
		1. Для работы синхронизации создайте специального пользователя mrsync
		2. Домашний каталог данного пользователя должен быть расположен в /opt/sync/. Данный каталог используйте как каталог синхронизации
		3. Домашний каталог не должен содержать никакой посторонней информации.
		4. Для выполнения синхронизации создайте rsync-пользователя sync c паролем parol666.
		5. Подключение к rsyncd должны быть разрешены исключительно от клиента L-CLI
	2. В качестве клиентов используются L-CLI
		1. Синхронизируемый каталог располагается по адресу /root/sync/
		2. Каталоги должны быть зеркально идентичны по содержимому.
		3. Реализуйте синхронизацию в виде скрипта:
			1. Скрипт находится по адресу /root/sync.sh
			2. Автоматизация скрипта реализована средствами cron пользователя root.

**Конфигурация параметров безопасности**

1. Настройте межсетевой экран **firewalld** на L-FW
	1. Запретите прямое попадание трафика из сети Интернет во внутренние сети
	2. Разрешите SSH подключения на соответствующий порт L-FW
	3. Разрешите необходимый трафик для доступности сайта www.skill39.wsr по протоколу HTTP из сети Интернет
	4. Разрешите необходимый трафик к серверу L-SRV по транслированным IP-адресам
	5. Остальные сервисы следует запретить.
		1. В отношении входящих (из внешней сети) ICMP запросов поступать по своему усмотрению

**Таблица 1** – DNS-имена

|  |  |
| --- | --- |
| **Хост** | **DNS-имя** |
| L-CLI | A,PTR: l-cli.skill39.wsr |
| L-SRV | A,PTR: l-srv.skill39.wsrCNAME: server.skill39.wsr |
| L-FW | A: l-fw.skill39.wsr |
| L-FW глобальный IP | A: www.skill39.wsr |

**Таблица 2** – 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

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

Версия 1 от 31.08.19.

## ВВЕДЕНИЕ

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

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.

**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.**

ДИАГРАММА ВИРТУАЛЬНОЙ СЕТИ 

**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 компании.

**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;

**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.

**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 c DC1 все зоны прямого и обратного просмотра;
* на SRV1 не должно быть основных зон прямого просмотра.

**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.

# Модуль С: «Пусконаладка телекоммуникационного оборудования»

Версия 4 от 31.07.19.

## 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 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 офиса HQ. Вы не имеете доступа к оборудованию провайдера, оно полностью настроено и не требует дополнительного конфигурирования. Вам необходимо настраивать оборудование предприятия, а именно: SW1, SW2, SW3, HQ1.

**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)

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 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 – **192.168.3.10**

SW2 – **192.168.3.20**

SW3 – **192.168.3.30**

HQ1 – **192.168.3.1**

1. **Базовая настройка**
2. Задайте имя всех устройств в соответствии с топологией.
3. Назначьте для всех устройств доменное имя **worldskills.ru**
4. Создайте на всех устройствах пользователей **wsruser** с паролем **network**
	1. Пароль пользователя должен храниться в конфигурации в виде результата хэш-функции.
	2. Пользователь должен обладать максимальным уровнем привилегий.
5. На всех устройствах установите пароль **wsr** на вход в привилегированный режим.
	1. Пароль должен храниться в конфигурации в виде результата хэш-функции.
6. Настройте режим, при котором все пароли в конфигурации хранятся в зашифрованном виде.
7. Для всех устройств реализуйте модель AAA (по возможности).
	1. Аутентификация на линиях виртуальных терминалов с 0 по 15 должна производиться с использованием локальной базы учётных записей.
	2. После успешной аутентификации при удалённом подключении пользователи сразу должен получать права, соответствующие их уровню привилегий или роли.
	3. Настройте необходимость аутентификации на локальной консоли.
	4. При успешной аутентификации на локальной консоли пользователи должны сразу должен получать права, соответствующие их уровню привилегий или роли.
8. На устройствах, к которым разрешен доступ, в соответствии с топологиями L2 и L3, создайте виртуальные интерфейсы, подинтерфейсы и интерфейсы типа петля, назначьте IP-адреса.
9. Все устройства должны быть доступны для управления по протоколу SSH версии 2.
10. **Настройка коммутации**
11. Для централизованного конфигурирования VLAN в коммутируемой сети предприятия используйте протокол VTP.
	1. В качестве сервера VTP настройте SW1.
	2. Коммутаторы SW2 и SW3 настройте в качестве VTP клиента.
	3. Таблица VLAN должна содержать следующие сети:
12. VLAN100 с именем **MGT**.
13. VLAN200 с именем **DATA**.
14. VLAN300 с именем **OFFICE**.
15. VLAN500 с именем **NATIVE**.
16. VLAN600 с именем **SHUTDOWN**.
17. Между всеми коммутаторами настройте транки с использованием протокола IEEE 802.1q.
18. Порты F0/10 коммутаторов SW2 и SW3, а также порт F0/1 коммутатора SW1 должны работать без использования согласования. Отключите протокол DTP явным образом.
19. Транк между коммутаторами SW2 и SW3 должен быть настроен без использования согласования. Отключите протокол DTP явным образом.
20. 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.
21. Для всех магистральных каналов назначьте native vlan 500.
22. Запретите пересылку по магистральным каналам все неиспользуемые VLAN, в том числе VLAN1
23. Настройте агрегирование каналов связи между коммутаторами.
24. 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);

1. Агрегированный канал между SW1 и SW2 должен быть организован с использованием протокола согласования LACP. SW1 должен быть настроен в активном режиме, SW2 в пассивном.
2. Агрегированный канал между SW1 и SW3 должен быть организован с использованием протокола согласования PAgP. SW1 должен быть настроен в предпочтительном, SW3 в автоматическом.
3. Конфигурация протокола остовного дерева:
4. Используйте протокол PVST.
5. Коммутатор SW1 должен являться корнем связующего дерева в сетях VLAN 100, 200 и 300, в случае отказа SW1, корнем должен стать коммутатор SW2.
6. Настройте порт F0/1 коммутатора SW1, таким образом, что при включении он сразу переходил в состояние forwarding не дожидаясь пересчета остовного дерева.
7. Настройте порт F0/10 коммутатора SW2 в соответствии с L2 диаграммой. Порты должен быть настроен в режиме доступа.
8. На всех устройствах, отключите неиспользуемые порты.
9. На всех коммутаторах, неиспользуемые порты переведите во VLAN 600.
10. **Настройка подключений к глобальным сетям**
	1. Настройте подключение PPPoE между ISP и маршрутизатором HQ1.
		1. Настройте PPPoE клиент на HQ1.
		2. Используйте имя пользователя **cisco** и пароль **cisco**
		3. HQ1 должен автоматически получать адрес от ISP.
11. **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. |

1. В офисе HQ, на устройстве HQ1 настройте протокол динамической маршрутизации OSPF.
	1. Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
	2. Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.
2. **Настройка служб**
3. В сетевой инфраструктуре сервером синхронизации времени является ISP. Все остальные сетевые устройства должны использовать его в качестве сервера времени.
	1. Передача данных между осуществляется без аутентификации.
	2. Настройте временную зону с названием MSK, укажите разницу с UTC +3 часов.
4. Настройте динамическую трансляцию портов (PAT):
	1. На маршрутизаторе HQ1 настройте динамическую трансляцию портов (PAT) для сети 192.168.3.0/24 в адрес петлевого интерфейса.
5. Настройте протокол динамической конфигурации хостов со следующими характеристиками
6. На маршрутизаторе HQ1 для подсети OFFICE:
7. Адрес сети – 192.168.3.0/24.
8. Адрес шлюза по умолчанию интерфейс роутера HQ1.
9. Адрес TFTP-сервера 172.16.0.10.
10. **Настройка механизмов безопасности**
11. На маршрутизаторе HQ1 настройте пользователей с ограниченными правами.
	1. Создайте пользователей **user1** и **user2** с паролем **cisco**
	2. 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**.
	3. Создайте и назначьте view-контекст **sh\_view** на пользователя **user2**
12. Команду show cdp neighbor
13. Все команды show ip \*
14. Команду ping
15. Команду traceroute
	1. Убедитесь, что пользователи не могут выполнять другие команды в рамках присвоенных контекстов и уровней привилегий.
16. На порту F0/10 коммутатора SW2, включите и настройте Port Security со следующими параметрами:
17. не более 2 адресов на интерфейсе
18. адреса должны динамически определяться, и сохраняться в конфигурации.
19. при попытке подключения устройства с адресом, нарушающим политику, на консоль должно быть выведено уведомление, порт не должен быть отключен.
20. На коммутаторе SW2 включите DHCP Snooping для подсети OFFICE. Используйте флеш-память в качестве места хранения базы данных.
21. На коммутаторе SW2 включите динамическую проверку ARP-запросов в сети OFFICE.
22. На маршрутизаторе HQ1 настройте расширенный список контроля доступа для подсети 192.168.3.0/24. Заблокируйте весь исходящий и входящий трафик от подсети 192.168.3.0/24 в интернет за исключением:
	1. Разрешите работу с DNS сервером 8.8.8.8.
	2. Разрешите исходящий TCP трафик по портам 80 и 443.
	3. Разрешите входящий трафик по TCP, только для тех соединений, если узел из подсети 192.168.3.0/24 инициирует это соединение.

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 24.

**Таблица 2 – Критерии оценки**

|  |  |  |
| --- | --- | --- |
| Раздел | Критерий | Оценки |
| Субъективная (если это применимо) | Объективная | Общая |
| А | Модуль А: «Пусконаладка инфраструктуры на основе OC семейства Linux» | 0 | 8 | 8 |
| В | Модуль В: «Пусконаладка инфраструктуры на основе OC семейства Windows» | 0 | 8 | 8 |
| С | Модуль С: «Пусконаладка телекоммуникационного оборудования» | 0 | 8 | 8 |
| Итого =  | 0 | 24 | 24 |

**5. ПРИЛОЖЕНИЯ К ЗАДАНИЮ**

1. <https://nextcloud.wsr39.ru/index.php/s/Gt7TagrrEwFjxj5> *-- Additional ISO Windows*
2. <https://nextcloud.wsr39.ru/index.php/s/ZRbYDLCPrRfEWjN> -- Additional ISO Linux
3. <https://nextcloud.wsr39.ru/index.php/s/KK8R2a9aBxNTJN2> -- Windows OVA
4. <https://nextcloud.wsr39.ru/index.php/s/aZLom2rXzjxQsCz> -- Linux OVA
5. <https://drive.google.com/file/d/1nYKF9P_zoWNAVcBaJCZ80f95vuTwfzti/view> -- Файлы предварительной конфигурации для Cisco
6. <https://nextcloud.wsr39.ru/index.php/s/TYm8jCjpcgGySSH> -- SRV1 Cisco OVA
7. <https://drive.google.com/file/d/17geWwpbCxa77cE2iQVFB1HKUti1KZx5a/view?usp=sharing> Набор диаграмм Cisco
8. <https://drive.google.com/file/d/1LW2QlWtVbwqfPieYUjCgpfzLaq1ZOYAs/view?usp=sharing> Диаграмма сети Linux
9. <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 применяемых операционных систем**

|  |  |
| --- | --- |
| **Имя компьютера** | **Операционная система** |
| DC1 | Windows Server 2016 GUI |
| SRV1 | Windows Server 2016 Core |
| CLI1 | Windows 10 Enterprise |
| DCA | Windows Server 2016 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.