# КОМПЕТЕНЦИЯ «СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

# КОНКУРСНОЕ ЗАДАНИЕ

# МОДУЛЬ С: ПУСКО-НАЛАДКА ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ

**Разработано экспертами WSR:**
**Горбачев А.П.**
**Щербинин А.А.**

**Дата: 17.09.17**
**Версия: 11**

Данное конкурсное задание состоит из следующих документов\файлов:
1. RC1718_TP39_Module-C_RU.docx
2. RC1718_TP39_Module-C-Topology_RU.vsd
3. RC1718_TP39_Module-C_Random_Generator.xlsx
4. RC1718_TP39_Module-C_Proposed_Changes.docx

# 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, CCNA Security. Задание разбито на следующие секции:

- Базовая настройка
- Настройка коммутации
- Настройка подключений к глобальным сетям
- Настройка маршрутизации
- Настройка служб
- Настройка механизмов безопасности
- 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 Frame-Relay и PPPoE 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. 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.

# НЕОБХОДИМОЕ ОБОРУДОВАНИЕ, ПРИБОРЫ, ПО И МАТЕРИАЛЫ

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

# 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.

**Базовая настройка**

1. Задайте имена ВСЕХ устройств в соответствии с топологией
2. Назначьте для ВСЕХ устройств доменное имя **wsr2018.ru**
3. Создайте на ВСЕХ устройствах пользователя **wsr2018** с паролем **cisco**
    a. Пароль пользователя должен храниться в конфигурации в виде результата хэш-функции.
    b. Пользователь должен обладать максимальным уровнем привилегий.
4. Для ВСЕХ устройств реализуйте модель AAA.
    a. Аутентификация на удаленной консоли должна производиться с использованием локальной базы данных
    b. После успешной аутентификации при входе с удаленной консоли пользователь сразу должен попадать в режим с максимальным уровнем привилегий.
    c. Настройте необходимость аутентификации на локальной консоли.
    d. При успешной аутентификации на локальной консоли пользователь должен попадать в режим с минимальным уровнем привилегий.
    e. 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.
    a. Пароль должен храниться в конфигурации НЕ в виде результата хэш-функции.
    b. Настройте режим, при котором все пароли в конфигурации хранятся в зашифрованном виде.
6. На ВСЕХ устройствах создайте виртуальные интерфейсы, подынтерфейсы и интерфейсы типа петля. Назначьте IP-адреса в соответствии с Таблицами 1 и 2.
    a. Для коммутаторов SW1, SW2 и SW3 создайте виртуальные интерфейсы в ВЛВС 101.
    b. Созданным виртуальным интерфейсам присвойте IP-адреса .51, .52 и .53 из подсети LAN соответственно.
    c. Включите механизм SLAAC для выдачи IPv6-адресов в сети LAN на интерфейсе маршрутизатора HQ1.
    d. На ВСЕХ коммутаторах отключите ВСЕ неиспользуемые порты.
7. Все устройства должны быть доступны для управления по протоколу SSH версии 2.
8. На маршрутизаторе HQ1 установите правильное время с учётом часового пояса.

**Настройка коммутации**

1. На ВСЕХ коммутаторах создайте ВЛВС:
    a. под номером 101 с именем LAN.
    b. под номером 102 с именем VOICE.
    c. под номером 103 с именем EDGE.
2. На коммутаторах SW1, SW2 и SW3 выполните настройку протокола динамического согласования транков (DTP).
    a. На коммутаторе SW3 переведите порты в Fa0/4-9 в режим, при котором коммутатор на данных портах будет инициировать согласование параметров транка.
    b. Переведите порты Fa0/7-9 на SW1 и Fa0/4-6 на SW2 в режим, при котором каждый коммутатор ожидает начала согласования параметров от соседа, но сам не инициирует согласование.

c. Переведите порты Fa0/1-3 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.
   a. Номера портовых групп:
      i. 1 — между коммутаторами SW1 <-> SW2;
      ii. 2 — между коммутаторами SW2 <-> SW3;
      iii. 3 — между коммутаторами SW3 <-> SW1.
   b. Коммутатор SW3 должен быть настроен в режиме активного согласования по обеим портовым группам по протоколу LACP;
   c. Коммутаторы SW1 и SW2 должны быть настроены в пассивном режиме LACP с коммутатором SW3.
   d. Коммутатор SW2 должен быть настроен в режиме активного согласования по протоколу PAgP с коммутатором SW1.
   e. Коммутатор SW1 должен быть настроен в режиме пассивного согласования по протоколу PAgP с коммутатором SW2.
4. Конфигурация протокола остовного дерева:
   a. На всех коммутаторах используйте вариант протокола STP, совместимый со стандартом 802.1w.
   b. Коммутатор SW1 должен являться корнем связующего дерева в VLAN 101. В случае его отказа, корнем должен стать коммутатор SW2. В случае отказа SW2 — коммутатор SW3.
   c. Коммутатор SW2 должен являться корнем связующего дерева в VLAN 102. В случае его отказа, корнем должен стать коммутатор SW3. В случае отказа SW3 — коммутатор SW1.
   d. Коммутатор SW3 должен являться корнем связующего дерева в VLAN 103. В случае его отказа, корнем должен стать коммутатор SW1. В случае отказа SW1 — коммутатор SW2.
   e. На коммутаторах SW1, SW2 и SW3 в VLAN 101, 102 и 103 используйте для передачи данных порты, не состоящие в портовых группах. В случае неисправности этих портов передача данных должна происходить через соответствующие агрегированные каналы.
5. На порту Fa0/5 коммутатора SW1 включите защиту от атаки на смену корня остовного дерева. При получении информации о том, что на этом порту находится потенциальный корень дерева в VLAN 101, порт должен переводиться в состояние root-inconsistent.
6. Настройте порт Fa0/10 коммутатора SW1 таким образом, чтобы порт переходил в состояние Forwarding, не дожидаясь пересчета остовного дерева.
7. Трафик сети LAN между HQ1 и SW3 должен передаваться без тэга IEEE 802.1Q

**Настройка подключений к глобальным сетям**

1. На маршрутизаторе HQ1 настройте PPP для подключения к маршрутизатору ISP. Для аутентификации используйте протокол CHAP с паролем cisco.
2. На маршрутизаторе BR3 настройте подключение к ISP через PPPoE.
   a. Используйте протокол PAP для аутентификации
   b. Используйте учетную запись cisco\cisco

c. Аутентификация должна быть двусторонней (клиент и сервер проверяют подлинность друг друга).
d. Настройте корректное значение MTU.

3. На маршрутизаторе HQ1 настройте IP SLA для проверки работоспособности Интернет-канала со следующими параметрами:
   a. Цель – 8.8.8.8
   b. Тип – эхо-запросы
   c. Частота – раз в 2 минуты
   d. Таймаут – 2 секунды

**Настройка маршрутизации**

1. На маршрутизаторах ISP, HQ1 и BR3 настройте протокол динамической маршрутизации EIGRP с номером автономной системы 2018.
   a. Включите маршрутизацию для сетей INET1, INET3, а также на интерфейсе Loopback100 маршрутизатора HQ1 и на интерфейсах Loopback101 и Loopback102 маршрутизатора BR3.
   b. Используйте алгоритм аутентификации md5 с ключом WSR.
   c. Настройте суммаризацию для сетей на интерфейсах Loopback101 и Loopback102 маршрутизатора BR3 таким образом, чтобы BR3 анонсировал вместо этих двух сетей только одну суммарную сеть минимально возможного размера.
   d. Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.
2. На маршрутизаторах HQ1 и BR3 настройте протокол динамической маршрутизации OSPFv3 с номером процесса 1.
   a. Используйте область с номером 0.
   b. Включите в обновления маршрутизации сети LAN, Loopback101 и Loopback103.
   c. Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.
3. На маршрутизаторах ISP, HQ1 и BR3 настройте протокол динамической маршрутизации BGP.
   a. Номера автономных систем 65000, 65001 и 65003 для ISP, HQ1 и BR3 соответственно.
   b. Включите в обновления маршрутизации сети на следующих интерфейсах:
      i. Loopback101 на HQ1,
      ii. Loopback101 и Loopback102 на ISP,
      iii. Loopback103 на BR3.
4. Оптимизируйте сходимость протоколов OSPF и EIGRP.
   a. Для протокола EIGRP настройте интерфейсы между маршрутизаторами так, чтобы hello-пакеты отправлялись раз в секунду, а соседство считалось недействительным после 4 пропущенных hello-пакетов.
   b. Для протокола OSPF настройте интерфейсы между маршрутизаторами так, чтобы соседство разрывалось после 15 секунд простоя, и за эти 15 секунд маршрутизатор должен бы был отправить 3 hello-пакета.

**Настройка служб**

1. Назначьте в качестве сервера синхронизации времени маршрутизатор HQ1.
    a. Настройте временную зону с названием MSK, укажите разницу с UTC +3 часа.
    b. Настройте сервер синхронизации времени. Используйте стратум 2.
    c. Настройте маршрутизатор BR3 в качестве клиента NTP
    d. Используйте аутентификацию MD5 с ключом WSR
2. На маршрутизаторе HQ1 настройте динамическую трансляцию портов (PAT) для устройств из сети LAN в адрес интерфейса, подключенного к сети INET1.
3. Настройте сервер DHCP со следующими характеристиками
    a. На маршрутизаторе HQ1 для подсети LAN:
        i. адрес сети – согласно таблице 1.
        ii. адрес шлюза по умолчанию — адрес интерфейса HQ1 в данной подсети
        iii. адрес сервера службы доменных имен — 8.8.8.8
        iv. исключите из раздачи адреса с .1 по .99.

**Настройка механизмов безопасности**

1. На маршрутизаторе BR3 настройте пользователей с ограниченными правами.
    a. Создайте пользователей user1 и user2 с паролем cisco.
    b. Пользователь user1 должен быть авторизован выполнять все команды пользовательского режима, а также иметь возможность осуществлять перезагрузку, включать и выключать отладку и удалять стартовую конфигурацию.
    c. Создайте view-контекст “show_view”. Включите в него
        i. Команду show version
        ii. Все команды show ip *
        iii. Команду who
    d. Создайте view-контекст “ping_view”. Включите в него
        i. Команду ping
        ii. Команду traceroute
    e. Создайте superview-контекст, объединяющий эти 2 контекста. При входе на маршрутизатор пользователь user2 должен попадать в данный контекст
    f. Убедитесь, что пользователи не могут выполнять другие команды в рамках присвоенных контекстов и уровней привилегий.
2. На порту коммутатора SW1, к которому подключен PC1, включите и настройте Port Security со следующими параметрами:
    a. не более 2 адресов на интерфейсе
    b. адреса должны динамически пополняться, но не сохраняться в текущей конфигурации
    c. при попытке подключения устройства с адресом, нарушающим политику, на консоль должно быть выведено уведомление, порт не должен быть отключен.
3. На коммутаторе SW1 включите DHCP-snooping для подсети LAN. Используйте флеш-память в качестве места хранения базы данных
4. На коммутаторе SW1 включите динамическую проверку ARP-запросов в сети LAN.
5. На коммутаторе SW3 настройте зеркалирование трафика, проходящего через порт 0/21 в оба направления, на порт 0/11.
6. На маршрутизаторе HQ1 настройте на интерфейсе, ведущем в сторону провайдера ISP, входящий список контроля доступа со следующими свойствами:

a. ACL должен позволять пользователям сети LAN выходить в Интернет, например заходить на сайт www.worldskills.ru **(Примечание**: для проверки включите на маршрутизаторе ISP веб-сервер и DNS-сервер командами **ip http server** , **ip http secure-server** , **ip dns server** , а также задайте статическую запись **ip host www.worldskills.ru 8.8.8.8** . Неработающий веб-сервер или DNS-сервер не позволят проверить выполнение этого условия.)
b. ACL должен разрешать другие виды трафика, необходимые для нормальной работы сети и сервисов.
c. ACL должен позволять отправлять эхо-запросы из внутренней сети и получать на них ответы.
d. Помимо указанных выше трёх видов все другие виды трафика должны быть запрещены. Попытки установить соединение с узлами сети LAN из внешних сетей должны быть максимально ограничены.

**Конфигурация виртуальных частных сетей**

1. На маршрутизаторах HQ1 и BR3 настройте GRE-туннель:
   a. Используйте в качестве VTI интерфейс Tunnel100
   b. Используйте адресацию согласно таблице 2.
2. На маршрутизаторах HQ1 и BR3 настройте IKEv1 IPsec Site-to-Site VPN и примените его к созданному GRE-туннелю
   a. Параметры политики первой фазы:
      i. Проверка целостности – MD5
      ii. Шифрование – DES
      iii. Группа Диффи-Хэлмана – 5
   b. Параметры преобразования трафика для второй фазы:
      i. Протокол – ESP
      ii. Шифрование – DES
      iii. Проверка целостности – MD5

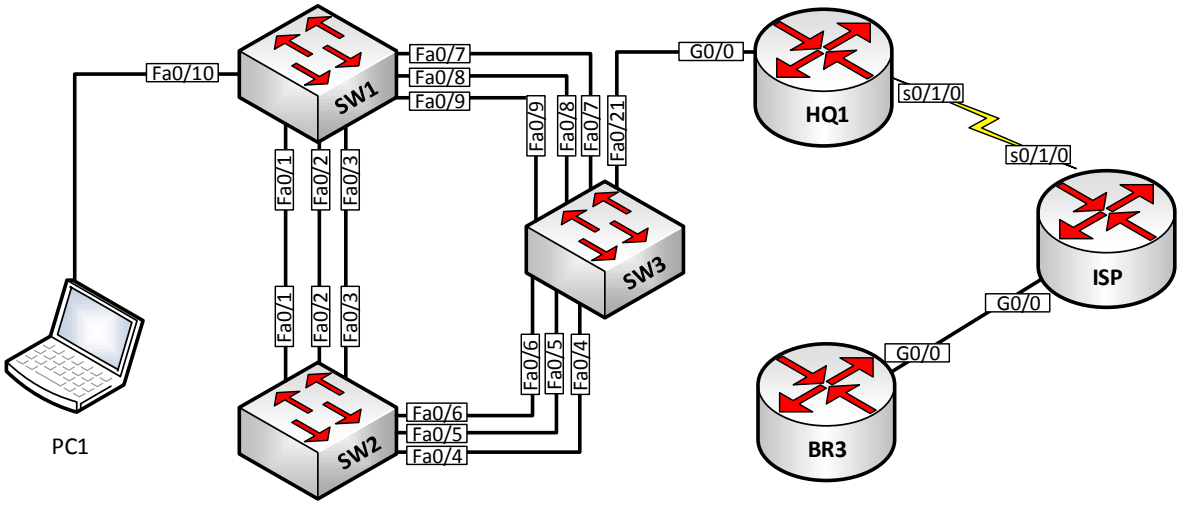
| Устройство | Интерфейс (Сеть) | IPv4-адрес |
|---|---|---|
| HQ1 | G0/0 (LAN) | 172.16.138.254/24 |
| | s0/1/0 (INET1) | 20.18.64.2/29 |
| | Loopback101 | 11.11.11.11/32 |
| | Tunnel100 | - |
| | | |
| ISP | s0/1/0 (INET1) | 20.18.64.1/29 |
| | VT1 (INET3) | 20.18.64.13/29 |
| | Loopback100 | 8.8.8.8/32 |
| | Loopback101 | 33.136.0.1/16 |
| | Loopback102 | 161.66.0.1/16 |
| | | |
| BR3 | Dialer1 (INET3) | 20.18.64.14/29 |
| | Loopback101 | 192.168.33.254/24 |
| | Loopback102 | 192.168.34.254/24 |
| | Loopback103 | 3.3.3.3/32 |
| | Tunnel100 | - |

**Таблица 1. IPv4-адресация**

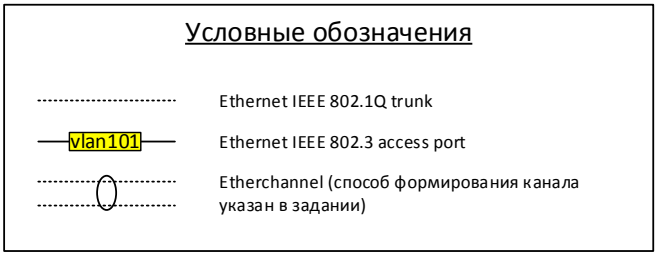
| Устройство | Интерфейс (Сеть) | IPv6-адрес |
|---|---|---|
| HQ1 | G0/0 (LAN) | 2018:218A:4021::1/64 |
| | s0/1/0 (INET1) | - |
| | Loopback101 | dead:beef::1/128 |
| | Tunnel100 | 2018::1/64 |
| | | |
| BR3 | Dialer1 (INET3) | - |
| | Loopback101 | - |
| | Loopback102 | - |
| | Loopback103 | dead:beef::3/128 |
| | Tunnel100 | 2018::2/64 |

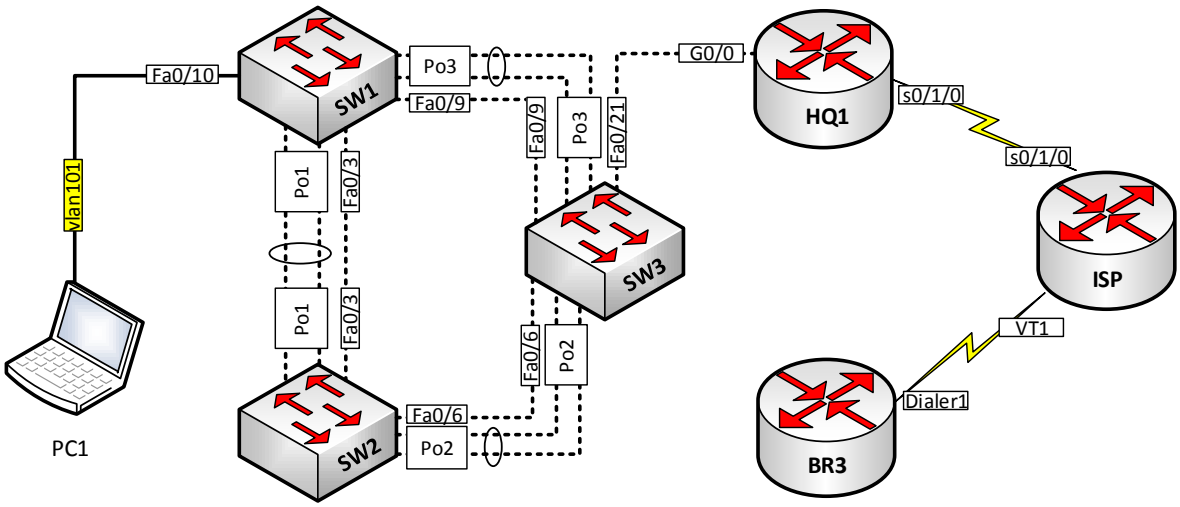
**Таблица 2. IPv6-адресация**

# Топология L1




# Топология L2



# Топология L3