«УТВЕРЖДЕНО»

КОНКУРСНОЕ ЗАДАНИЕ

по компетенции «Сетевое и системное администрирование»
для проведения II регионального чемпионата
«Молодые профессионалы» (WorldSkills Russia)
Рязанской области 2018

Рязань, 2018

«СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

КОНКУРСНОЕ ЗАДАНИЕ

МОДУЛЬ А: ПУСКО-НАЛАДКА ИНФРАСТРУКТУРЫ НА ОСНОВЕ ОС СЕМЕЙСТВА LINUX

РАЗРАБОТАНО ЭКСПЕРТОМ WSR: ФУЧКО М.М.

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 служб хранения данных
- Конфигурация параметров безопасности и служб аутентификации

Секции независимы друг от друга, но вместе они образуют достаточно сложную инфраструктуру. Некоторые задания достаточно просты и понятны, некоторые могут быть неочевидными. Можно заметить, что некоторые технологии должны работать в связке или поверх других технологий. Например, динамическая маршрутизация должна 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. Например, задание 6 в секции «Базовая конфигурация» предписывает автоматизировать удаленный доступ, который, разумеется, не будет работать без предварительной конфигурации, изложенной в секции «Маршрутизация и удаленный доступ». 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.

Виртуальная машина ISPSRV преднастроена. Управляющий доступ участника к данной виртуальной машине для выполнения задания не предусмотрен.

НЕОБХОДИМОЕ ОБОРУДОВАНИЕ, ПРИБОРЫ, ПО И МАТЕРИАЛЫ

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

КОМПЛЕКТАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Для выполнения конкурсного задания участникам должно быть предоставлено следующее программное обеспечение:

- CentOS 7 Everything;
- Пакеты, совместимые с используемой версией CentOS 7;
  - openvpn
  - easy-rsa
  - pkcs11-helper
  - pam_radius;

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

ОПИСАНИЕ ПРИМЕНЯЕМЫХ ОПЕРАЦИОННЫХ СИСТЕМ

Имя виртуальной машины	Операционная система
CLI-N	CentOS 7 (GUI)
CLI-C	CentOS 7 (GUI)
CLI-P	CentOS 7 (GUI)
RTR	CentOS 7 (Minimal)
ISP	CentOS 7 (Minimal)
SRV	CentOS 7 (Minimal)

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 **Таблицей 1.**
2) Установите следующее ПО на **ВСЕ** хосты:
    a. Пакет tcpdump
    b. Клиент ftp
    c. Клиент lftp
    d. Пакет net-tools
    e. Редактор vim
3) На хостах RTR, CLI-P, SRV, CLI-N, CLI-C сформируйте файл **/etc/hosts** в соответствии с **Таблицей 1** (кроме адреса хоста CLI-P). Данный файл будет применяться во время проверки в случае недоступности DNS-сервисов. Проверка по IP-адресам выполняться не будет. В случае корректной работы DNS-сервисов изменения в файлах **/etc/hosts** не требуются.

Конфигурация сетевой инфраструктуры

1) Настройте IP-адресацию на ВСЕХ хостах в соответствии с **Таблицей 1.**
2) Настройте сервер протокола динамической конфигурации хостов для машин CLI-C и CLI-P
    a. В качестве DHCP-сервера используйте машину SRV
    b. Используйте пул адресов 172.16.100.60 — 172.16.100.75
    c. Используете адрес машины SRV в качестве адреса DNS-сервера
    d. Настройте DHCP-сервер таким образом, чтобы машина CLI-C всегда получала фиксированный IP-адрес в соответствии с **Таблицей 1**
    e. В качестве шлюза по умолчанию используйте адрес интерфейса RTR в локальной сети
    f. Используйте DNS-суффикс **house.mad**
    g. DNS-записи типа A соответствующего хоста должны обновляться при получении им адреса от DHCP-сервера.
3) На машине SRV настройте службу разрешения доменных имен
    a. Сервер должен обслуживать зону **house.mad**
    b. Сопоставление имен организовать в соответствии с **Таблицей 2**
    c. Запросы, которые выходят за рамки зоны **house.mad** должны пересылаться DNS-серверу ISPSRV
    d. Реализуйте поддержку разрешения обратной зоны.
    e. Файлы зон располагать в **/opt/dns/**
4) На RTR настройте интернет-шлюз для организации коллективного доступа в интернет. Настройте трансляцию сетевых адресов из внутренней сети в адрес внешнего интерфейса.

Службы централизованного управления и журналирования

1) На SRV разверните RADIUS-сервер с использованием пакета freeradius для организации централизованного управления учетными записями
    a. Создайте учетные записи user01 … user50
    b. Учетные записи должны храниться в локальном файле **/etc/passwd**
    c. Настройте RTR, CLI-C и CLI-P в качестве клиентов RADIUS-сервера.
2) На SRV организуйте централизованный сбор журналов с хостов CLI-C, CLI-P и RTR.
    a. Журналы должны храниться в директории **/opt/logs/**
    b. Журналирование должно производится в соответствии с **Таблицей 3.**

Конфигурация служб удаленного доступа

1) На RTR настройте сервер удаленного доступа на основе технологии OpenVPN:
    a. В качестве сервера выступает RTR
    b. Параметры туннеля
        i. Устройство TUN
        ii. Протокол UDP
        iii. Применяется сжатие
        iv. Порт сервера 1122
    c. Ключевая информация должна быть сгенерирована на RTR
    d. Хранение всей необходимой (кроме конфигурационных файлов) информации организовать в **/opt/vpn**
2) На CLI-N настройте клиент удаленного доступа на основе технологии OpenVPN:
    a. Запуск удаленного подключения должен выполняться скриптом **start_vpn**
        i. Автоматизация отключения VPN-туннеля не требуется
        ii. Скрипт должен располагаться в **/opt/vpn**.
        iii. Скрипт должен вызываться из любого каталога без указания пути
        iv. Используйте следующий путь для расположения файла скрипта **/opt/vpn/start_vpn.sh**
3) На RTR настройте удаленный доступ по протоколу SSH:
    a. Доступ ограничен пользователями **ssh_p** и **ssh_c**
    b. SSH-сервер должен работать на порту **1022**
4) На CLI-N настройте клиент удаленного доступа SSH:
    a. Доступ к серверу RTR должен происходить автоматически по правильному порту, без его явного указания номера порта в команде подключения
    b. Для других серверов по умолчанию должен использоваться порт **22**
    c. Доступ к RTR под учетной записью **ssh_p** должен происходить с помощью аутентификации на основе открытых ключей.

Конфигурация служб хранения данных

1) На SRV настройте сервер файлового хранилища на основе технологии NFS:
    a. В качестве хранилища используется каталог **/opt/nfs**
    b. Доступ организуется для чтения и записи
2) Настройте автоматическое монтирование NFS-хранилища для клиентов CLI-C, CLI-P и CLI-N:
    a. Используйте DNS-имя NFS-сервера
    b. Используйте **/opt/nfs** в качестве пути для монтирования
    c. Клиенты CLI-C и CLI-P монтируют NFS-каталог при запуске ОС
    d. Клиент CLI-N монтирует NFS-каталог после установления VPN-туннеля с RTR
3) На SRV настройте FTP-сервер для доступа к файловому хранилищу
    a. Обеспечьте доступ для клиента CLI-N с использованием стандартных портов протокола FTP через внешний интерфейс маршрутизатора RTR
    b. Корень FTP-сервера должен располагаться в **/opt/nfs**
    c. Доступ должен быть ограничен пользователем ftpuser:ftppass с правами на чтение и запись

Конфигурация параметров безопасности и служб аутентификации

1) Настройте межсетевой экран на RTR
    a. Запретите прямое попадание трафика из сети **First Mile** в **Internal**
    b. Разрешите удаленные подключения с использованием OpenVPN на внешний интерфейс маршрутизатора RTR
    c. Разрешите SSH подключения на соответствующий порт

d. Разрешите подключения по FTP в соответствии с заданием
e. Для VPN-клиентов должен быть предоставлен полный доступ к сети **Internal**

Таблица 1. Адресация

Сеть	**Хосты**	**Адреса (/24)**
Internal	CLI-P CLI-C RTR SRV	DHCP 172.16.100.50 (DHCP) 172.16.100.1 172.16.100.100
Last Mile	ISP RTR	10.10.10.1 10.10.10.10
First Mile	ISP CLI-N	20.20.20.1 20.20.20.10

Таблица 2. DNS-имена

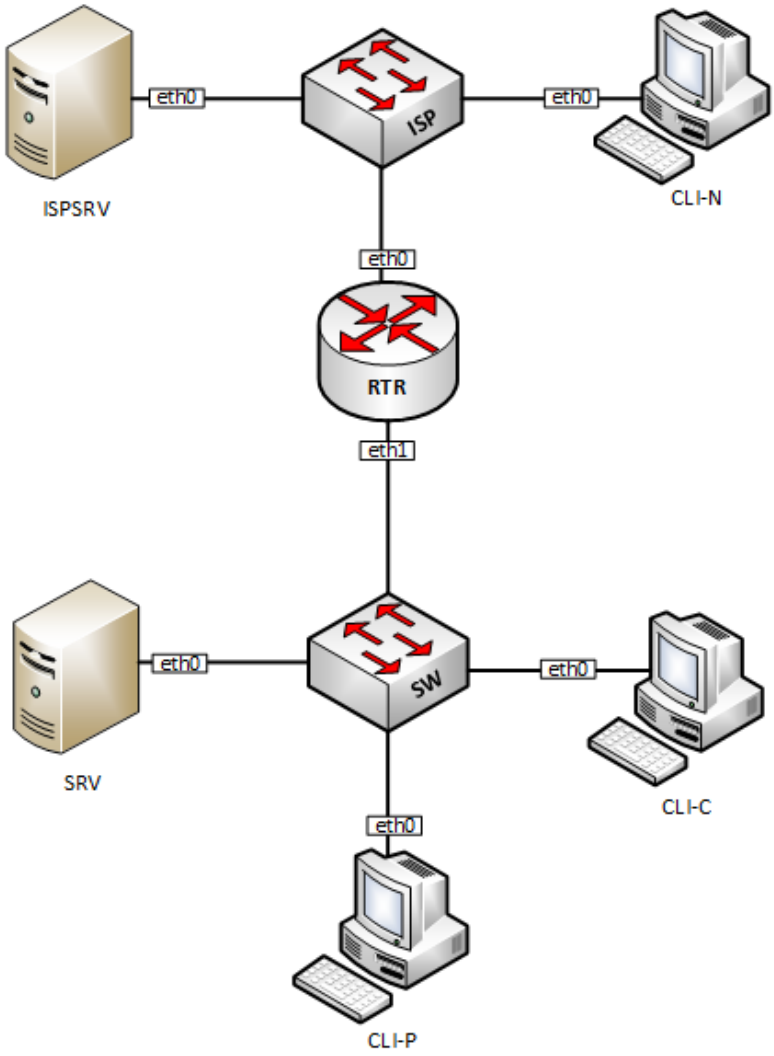
Хост	**DNS-имя**
CLI-P	A:cli-p.house.mad CNAME: mom.house.mad CNAME: dad.house.mad
CLI-C	A:cli-c.house.mad CNAME: son.house.mad
SRV	A:srv.house.mad CNAME: server.house.mad CNAME: center.house.mad
RTR	A:rtr.house.mad CNAME: fw.house.mad

Таблица 3. Правила журналирования

Источник	**Уровень журнала**	**Файл**
Все хосты	critical и выше	/opt/logs/<HOSTNAME>/crit.log
SRV	auth.*	/opt/logs/<HOSTNAME>/auth.log
RTR	*.err	/opt/logs/<HOSTNAME>/error.log
Все кроме RTR	*.err	/opt/logs/err.log

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

Диаграмма виртуальной сети



«СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

КОНКУРСНОЕ ЗАДАНИЕ

МОДУЛЬ В:
ПУСКО-НАЛАДКА ИНФРАСТРУКТУРЫ НА ОСНОВЕ ОС СЕМЕЙСТВА MICROSOFT WINDOWS

РАЗРАБОТАНО ЭКСПЕРТОМ WSR: ДЮГУРОВЫМ Д.В.

ВВЕДЕНИЕ

Умение работать с операционными системами семейства Microsoft Windows является 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

В рамках легенды конкурсного задания Вы – системный администратор вновь создаваемой московской компании. Вам необходимо настроить сервисы в локальной сети головного офиса.
Также учтите, что компания приобрела одно из малых предприятий в Ижевске. В ижевском офисе сеть уже функционировала, но системный администратор (из-за скандала при увольнении) не предоставил доступа к действующему там контроллеру домена. Вам придется восстановить доступ к ижевскому домену.
Также Вам предстоит настроить защищенный канал связи между офисами, доверие между доменами и удаленное подключение клиентов, предварительно смоделировав наличие провайдера Интернета.

ИНСТРУКЦИИ ДЛЯ УЧАСТНИКА

Для выполнения конкурсного задания вы должны обеспечить наличие и функционирование в соответствии с заданием служб и ролей на указанных виртуальных машинах. При вы можете самостоятельно выбирать способ настройки того или иного компонента, используя предоставленные вам ресурсы по своему усмотрению.
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.
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.

НЕОБХОДИМОЕ ОБОРУДОВАНИЕ, ПРИБОРЫ, ПО И МАТЕРИАЛЫ

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

КОМПЛЕКТАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Для выполнения конкурсного задания участникам должно быть предоставлено следующее программное обеспечение:

- Windows server 2016;
- Microsoft Office;
- RSAT tools for Windows 10;
- Windows10.ADMX.

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

ОПИСАНИЕ ПРИМЕНЯЕМЫХ ОПЕРАЦИОННЫХ СИСТЕМ

Имя виртуальной машины	Операционная система
DC-IZ	Windows Server 2016 GUI
CLIENT-IZ	Windows 10 Enterprise
IIS-IZ	Windows Server 2016 Core
EDGE-IZ	Windows Server 2016 GUI
DC-M	Windows Server 2016 GUI
FILES-M	Windows Server 2016 Core
SUBCA-M	Windows Server 2016 GUI
EDGE-M	Windows Server 2016 Core
CLIENT-M	Windows 10 Enterprise
ROOTCA-M	Windows Server 2016 GUI

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.

КОНКУРСНОЕ ЗАДАНИЕ

Настройка DC-M

Базовая настройка

- переименуйте компьютер в DC-M;
- задайте настройки сети в соответствии с таблицей 1;
- обеспечьте работоспособность протокола ICMP (для использования команды ping).

Active Directory

- сделайте сервер основным контроллером домена Moscow.ru;
- настройте одностороннее нетранзитивное доверие с доменом Izhevsk.ru – пользователи домена Moscow.ru должны иметь доступ к ресурсам домена Izhevsk.ru, но не наоборот.

DHCP

- настройте протокол DHCP для автоконфигурации клиентов;
- настройте failover: mode – Load balancer, partner server – FILES-M, state swithover – 10 min;
- диапазон выдаваемых адресов: 172.16.0.100-200/24;
- настройте дополнительные свойства области (адреса обоих DNS-серверов и основного шлюза).

DNS

- настройте необходимые зоны прямого и обратного просмотра, обеспечьте их согласованную работу со службой DNS на FILES-M;
- создайте вручную все необходимые записи типа A и PTR для серверов домена и необходимых web-сервисов;
- сделайте необходимые настройки для работоспособности доверия с доменом Izhevsk.ru (при появлении в сети новых DNS серверов они должны автоматически получать необходимые для работоспособности доверия настройки).

GPO

- запретите анимацию при первом входе пользователей в систему на всех клиентских компьютерах домена;
- члены группы IT должны быть членами группы локальных администраторов на всех клиентских компьютерах домена;
- в браузерах IE Explorer и Microsoft Edge (установите и используйте windows10.admx) должна быть настроена стартовая страница – www.moscow.ru;
- запретите изменение экранной заставки и *Корзину* на рабочем столе для всех пользователей домена, кроме членов группы локальных администраторов клиентских компьютеров;
- для членов группы Experts настройте перенаправление папок *my Documents* и *Desktop* по адресу FILES-M→d:\shared\redirected.

Элементы доменной инфраструктуры

- создайте подразделения: Experts, Competitors, Managers, Visitors, IT и Project;
- в соответствующих подразделениях создайте доменные группы: Experts, Competitors, Managers, Visitors, IT, Project_Budget-R, Project_Budget-W, Project_Intranet-R, Project_Intranet-W, Project_Logistics-R, Project_Logistics-W;

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 пользователей, используя прилагаемый excel-файл (вся имеющаяся в файле информация о пользователях должна быть внесена в Active Directory); поместите пользователей в соответствующие подразделения и группы; все созданные учетные записи должны быть включены и доступны;
- для каждого пользователя создайте автоматически подключаемую в качестве диска U:\ домашнюю папку по адресу FILES-M→d:\shares\users.

Настройка FILES-M

Базовая настройка

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

Active Directory

- сделайте сервер дополнительным контроллером домена Moscow.ru;
- контроллер не должен выполнять функцию глобального каталога.

DHCP

- настройте протокол DHCP для автоконфигурации клиентов;
- настройте failover: mode – Load balancer, partner server – DC-M, state swithover – 10 min;

DNS

- сделайте сервер дополнительным DNS-сервером в домене Moscow.ru;
- загрузите с DC-M все зоны прямого и обратного просмотра.

Общие папки

- создайте общие папки для подразделений (Competitors, Experts and Managers) по адресу FILES-M→d:\shares\departments;
- обеспечьте привязку общей папки подразделения к соответствующей группе в качестве диска G:\;
- создайте общую папку проектов по адресу FILES-M→d:\shares\projects;
- в папке d:\shares\projects создайте следующие папки: Budget, Intranet, Logistics; настройте разрешения этих папок в соответствии с таблицей 2;
- создайте привязку общей папки проектов для всех пользователей, кроме членов группы Visitors, в качестве диска P:\; пользователи должны видеть только те папки внутри диска P:\, к которым им разрешен доступ.

Квоты/Файловые экраны

- установите максимальный размер в 5Gb для каждой домашней папки пользователя (U:\);
- запретите хранение в домашних папках пользователей файлов с расширениями .cmd и .exe; учтите, что файлы остальных типов пользователи вправе хранить в домашних папках.

IIS

- создайте сайт для менеджеров компании (используйте предоставленный htm-файл в качестве документа по умолчанию);
- сайт должен быть доступен по имени managers.moscow.ru только по протоколу https исключительно для членов группы Managers по их пользовательским сертификатам.

Настройка ROOTCA-M

Базовая настройка

- переименуйте компьютер в ROOTCA-M;
- задайте настройки сети в соответствии с таблицей 1;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- не присоединяйте компьютер к какому-либо домену.

Службы сертификации

- установите службы сертификации;
- настройте одиночный корневой сервер сертификации (длина ключа и алгоритмы шифрования значения не имеют);
- имя центра сертификации – Moscow Root CA;
- срок действия сертификата – 10 лет;
- CRL location: http://RU-SUBCA.russia.net/certenroll/<caname><crlnamesuffix><deltacrlallowed>.crl
- AIA location: http://RU-SUBCA.russia.net/certenroll/<serverdnsname>_<caname><certificatename>.crt
- создайте список отзыва сертификатов и сертификат корневого центра сертификации для SUBCA-M;
- выпустите сертификат подчиненного центра сертификации для SUBCA-M, одобрив соответствующий запрос;
- после всех настроек отключите сетевой интерфейс.

Настройка SUBCA-M

Базовая настройка

- переименуйте компьютер в SUBCA-M;
- задайте настройки сети в соответствии с таблицей 1;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к домену Moscow.ru.

Службы сертификации

- установите службы сертификации;
- настройте подчиненный доменный центр сертификации;
- имя центра сертификации – Moscow Sub CA;
- срок действия сертификата – 5 лет;
- импортируйте и опубликуйте список отзыва сертификатов с ROOTCA-M;
- настройте шаблон выдаваемого сертификата для клиентских компьютеров *MoscowClients*: *subject name=common name*, автозапрос для всех клиентских компьютеров домена;
- настройте шаблон выдаваемого сертификата для группы Managers *MoscowUsers*: *subject name=common name*, автозапрос только для пользователей – членов группы Managers.

Настройка CLIENT-M

Базовая настройка

- переименуйте компьютер в CLIENT-M;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к домену Moscow.ru;
- установите набор компонентов удаленного администрирования RSAT;
- запретите использование «спящего режима»;
- используйте компьютер для тестирования настроек в домене Moscow.ru: пользователей, общих папок, групповых политик, в том числе – тестирования удаленных подключений через Direct Access (временно переключаю компьютер в сеть Internet).

Работа с DC-IZ

Восстановление доступа

- получите (восстановите) доступ к контроллеру домена и реплике Active Directory; помните – на сервере хранится важная информация, поэтому просто переустановить операционную систему нельзя!

Поиск пользователей и ресурсов

- найдите всех пользователей домена Izhevsk.ru, у которых в графе *Job Title* проставлено значение *Expert*;
- переместите всех найденных пользователей в специальное подразделение Migration (при необходимости создайте его) и отключите учетные записи в домене Izhevsk.ru;
- в домене Moscow.ru в подразделении Migrated (при необходимости создайте это подразделение) создайте новые учетные записи, соответствующие найденным ранее и отключенным учетным записям; задайте для них пароль *NewP@ssw0rd*;

DNS

- сделайте необходимые настройки для работоспособности доверия с доменом Moscow.ru (при появлении в сети новых DNS серверов они должны автоматически получать необходимые для работоспособности доверия настройки);
- обеспечьте разрешение имен сайтов www.moscow.ru и www.izhevsk.ru.

Службы удаленных рабочих столов

- разверните терминальный сервер, не устанавливайте и не настраивайте компоненты лицензирования;
- сконфигурируйте web-доступ RemoteApp к службам терминалов сервера;
- опубликуйте программу *Wordpad* на web-портале RemoteApp для членов группы Moscow\IT;
- опубликуйте программу *Notepad* на web-портале RemoteApp для членов группы Moscow\Managers;
- 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.izhevsk.ru и https://rds.izhevsk.ru;
- с помощью доменного центра сертификации на сервере SUBCA-M 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 Moscow.ru или Izhevsk.ru к сайту по имени https://rds.izhevsk.ru сертификат должен распознаваться как доверенный и действительный.

Работа с IIS-IZ

IIS

- создайте сайт www.moscow.ru (используйте предоставленный htm-файл в качестве документа по умолчанию);
- создайте сайт www.izhevsk.ru (используйте предоставленный htm-файл в качестве документа по умолчанию);
- оба сайта должны быть доступны по протоколу https с использованием сертификатов, выданных SUBCA-M.

Работа с CLIENT-IZ

Базовая настройка

- переименуйте компьютер в CLIENT-IZ;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к домену Izhevsk.ru;
- запретите использование «спящего режима»;
- используйте компьютер для тестирования настроек в домене Izhevsk.ru.

Настройка EDGE-IZ

Базовая настройка

- переименуйте компьютер в EDGE-IZ;
- задайте настройки сети в соответствии с таблицей 1;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к домену Izhevsk.ru.

Настройка RRAS

- установите службу RRAS;
- настройте статический маршрут в сеть 172.16.0.0 через «внешний интерфейс».

Настройка EDGE-M

Базовая настройка

- переименуйте компьютер в EDGE-M;
- задайте настройки сети в соответствии с таблицей 1;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к домену Moscow.ru.

Настройка RRAS

- установите службу RRAS;
- настройте статический маршрут в сеть 172.19.0.0 через «внешний интерфейс».

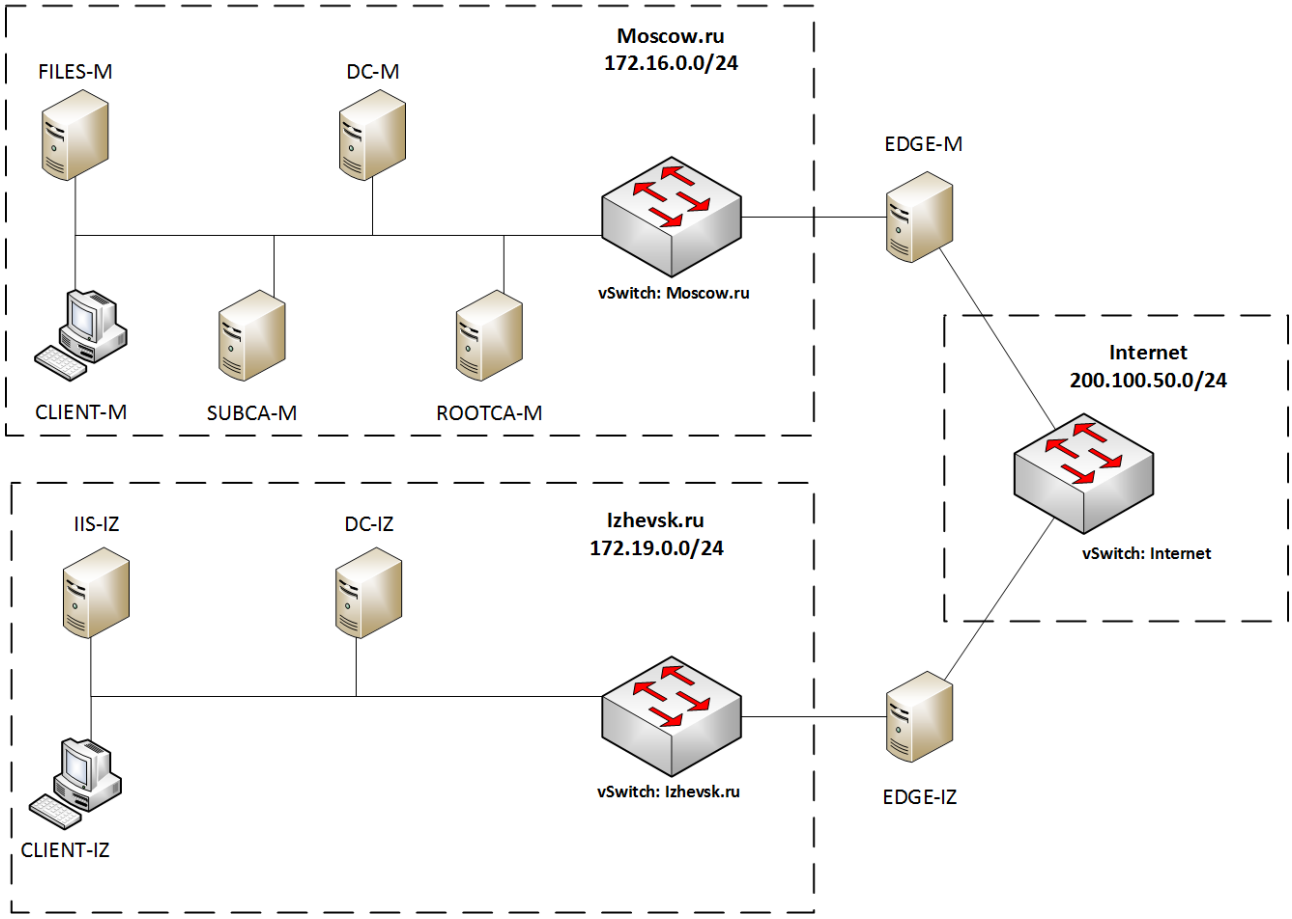
Таблица 1.

Имя компьютера	Имя домена	IP-адреса
DC-IZ	Izhevsk.ru	172.19.0.1/24
CLIENT-IZ		DHCP
IIS-IZ		172.19.0.3/24
EDGE-IZ		172.19.0.250/24 200.100.50.101/24
DC-M	Moscow.ru	172.16.0.1/24
FILES-M		172.16.0.2/24
SUBCA-M		172.16.0.4/24
EDGE-M		172.16.0.250/24 200.100.50.100/24
CLIENT-M		DHCP
ROOTCA-M	None	172.16.0.3/24

Таблица 2.

Имя общего ресурса	Расположение	Доступ только для чтения	Доступ для чтения и записи
Budget	FILES-M→D:\shares\projects	RU-Budget-R	RU-Budget-W
Intranet		RU-Intranet-R	RU-Intranet-W
Logistics		RU-Logistics-R	RU-Logistics-W

Диаграмма виртуальной сети



«СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

КОНКУРСНОЕ ЗАДАНИЕ

МОДУЛЬ С: ПУСКО-НАЛАДКА ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ

РАЗРАБОТАНО ЭКСПЕРТАМИ WSR:

Горбачев А.П.
Щербинин А.А.

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.

КОНКУРСНОЕ ЗАДАНИЕ

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

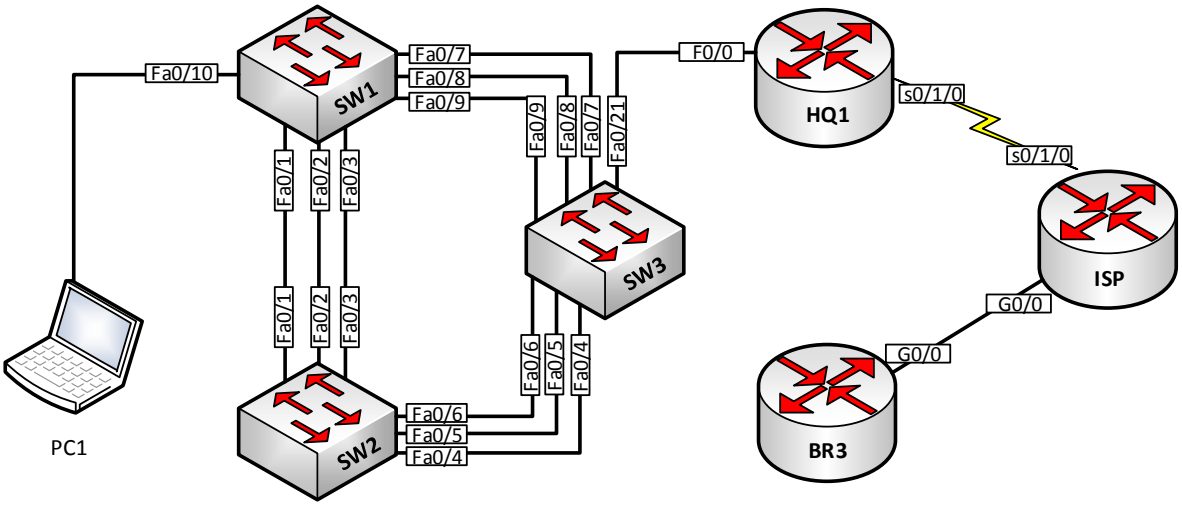
Устройство	Интерфейс (Сеть)	IPv4-адрес
HQ1	F0/0 (LAN)	172.16.138.254/24
	s0/1/0 (INET1)	20.18.64.2/29
	Loopback101	11.11.11.11/32
	Tunnel100	-
ISP	s0/1/0 (INET1)	20.18.64.1/29
	VT1 (INET3)	20.18.64.13/29
	Loopback100	8.8.8.8/32
	Loopback101	33.136.0.1/16
	Loopback102	161.66.0.1/16
BR3	Dialer1 (INET3)	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

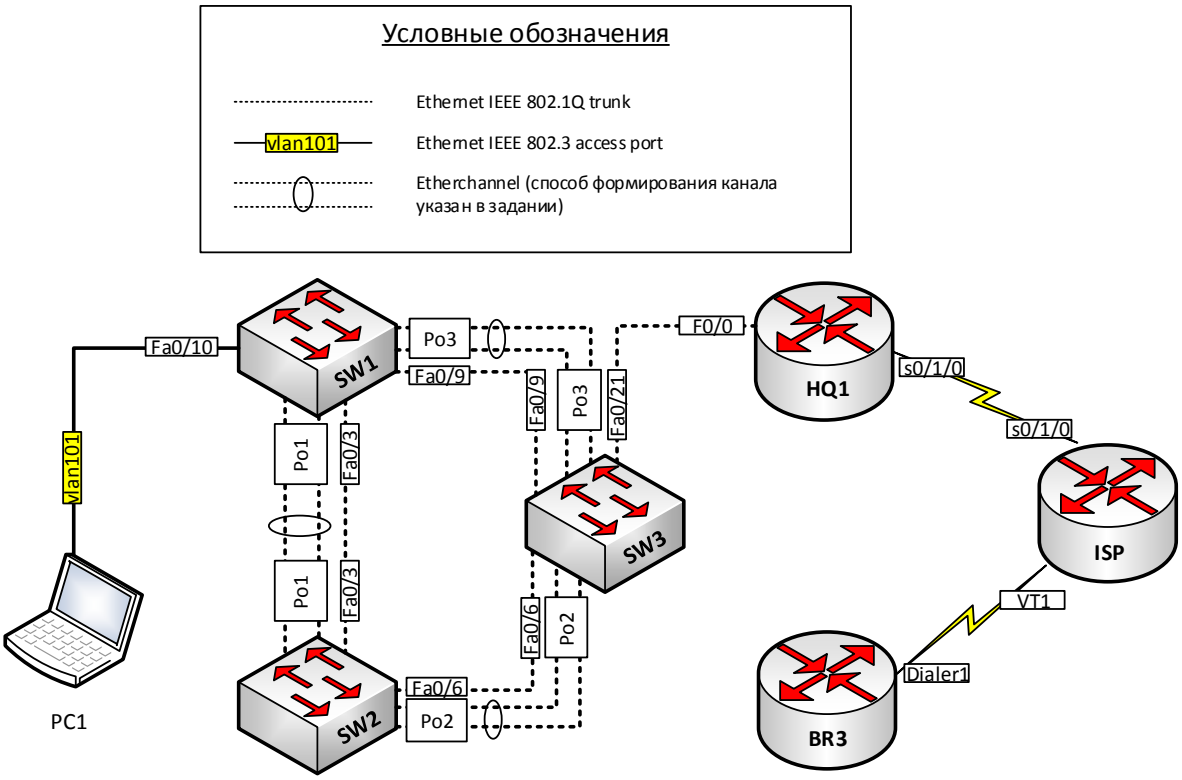
Устройство	Интерфейс (Сеть)	IPv6-адрес
HQ1	F0/0 (LAN)	2018:218A:4021::1/64
	s0/1/0 (INET1)	-
	Loopback101	dead:beef::1/128
	Tunnel100	2018::1/64
BR3	Dialer1 (INET3)	-
	Loopback101	-
	Loopback102	-
	Loopback103	dead:beef::3/128
	Tunnel100	2018::2/64

Таблица 2. IPv6-адресация

Топология L1



Топология L2



Топология L3

