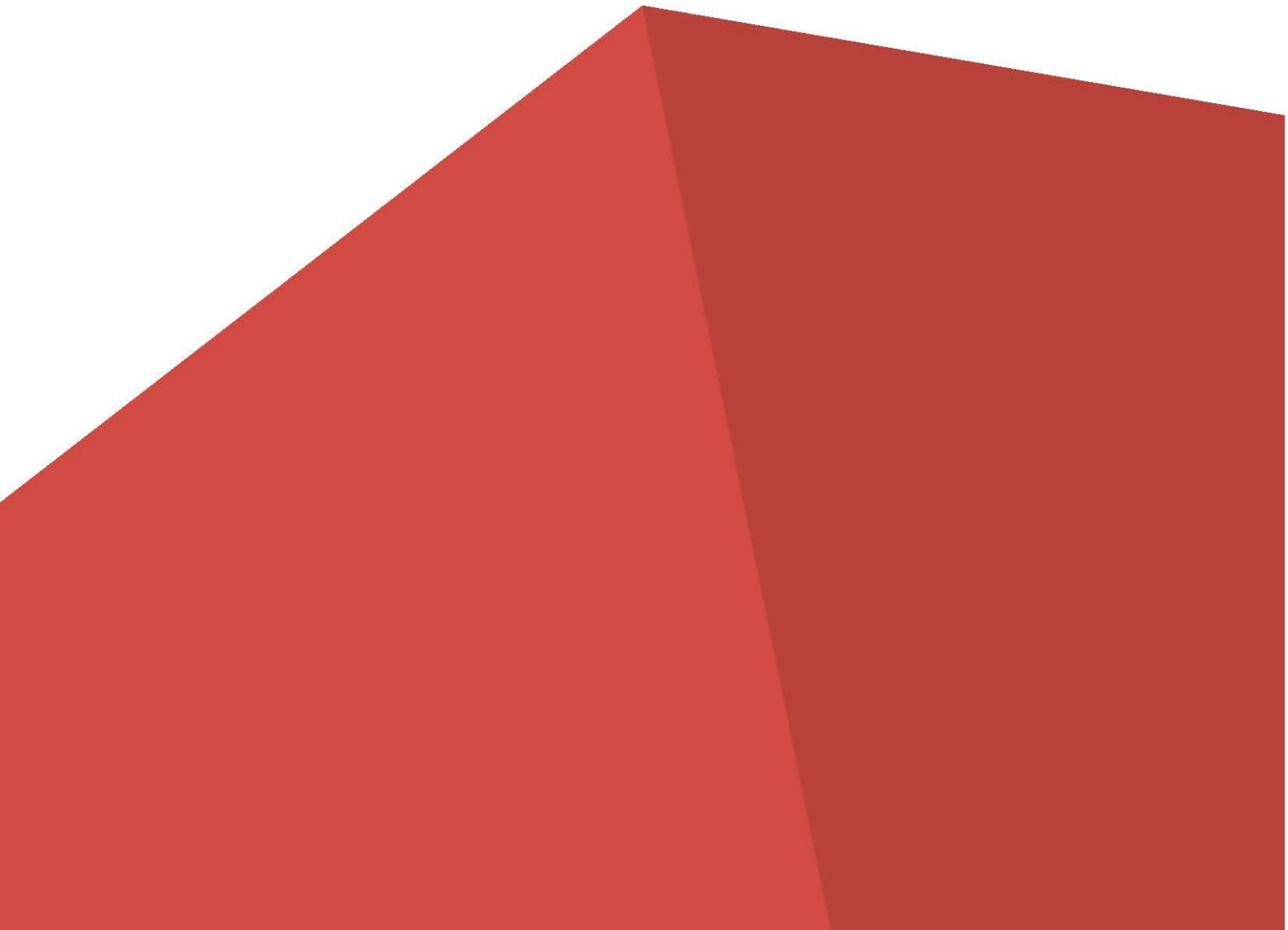
Конкурсное задание

Компетенция
КОМПЕТЕНЦИЯ «СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

Конкурсное задание включает в себя следующие разделы:

1. Формы участия в конкурсе
2. Задание для конкурса
3. Модули задания и необходимое время
4. Критерии оценки
5. Необходимые приложения

Количество часов на выполнение задания:15ч.



1. ФОРМЫ УЧАСТИЯ В КОНКУРСЕ

Индивидуальный конкурс.

2. ЗАДАНИЕ ДЛЯ КОНКУРСА

Содержанием конкурсного задания являются работы по пуско-наладке сетевой инфраструктуры на базе современного сетевого оборудования и операционных систем семейства Windows и Linux. Участники соревнований получают инструкцию, сетевые диаграммы и методические рекомендации по выполнению. Конкурсное задание имеет несколько модулей, выполняемых последовательно.

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

Конкурс включает в себя Пуско-наладку инфраструктуры на основе ОСсемейства Linux; Пуско-наладку инфраструктуры на основе ОСсемейства Windows; Пуско-наладку телекоммуникационного оборудования.

Окончательная методика проверки уточняются членами жюри. Оценка производится в отношении работы модулей. Если участник конкурса не выполняет требования техники безопасности, подвергает опасности себя или других конкурсантов, такой участник может быть отстранен от конкурса.

Время и детали конкурсного задания в зависимости от конкурсных условий могут быть изменены членами жюри, по согласованию с менеджером компетенции.

Конкурсное задание должно выполняться помодульно, циклически по модулям A-B-C. Оценка каждого модуля происходит Ежедневно.

3. МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ

Модули и время приедены в таблице 1

Таблица 1 – Время выполнение модуля

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

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

Версия 1Б от 27.09.18.

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 RedHat. Задания поделены на следующие секции:

- Базовая конфигурация
- Конфигурация сетевой инфраструктуры
- Службы централизованного управления и журналирования
- Конфигурация служб удаленного доступа
- Конфигурация веб служб
- Конфигурация служб хранения данных
- Конфигурация параметров безопасности и служб аутентификации

Секции независимы друг от друга, но вместе они образуют достаточно сложную инфраструктуру. Некоторые задания достаточно просты и понятны, некоторые могут быть неочевидными. Можно заметить, что некоторые технологии должны работать в связке или поверх других технологий. Например, динамическая маршрутизация должна 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 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. Например, задание 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.

Если Вам требуется установить пароль, не указанный 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.

Организация RIGHT включает виртуальные машины: R-FW, R-CLI, OUT-CLI.

НЕОБХОДИМОЕ ОБОРУДОВАНИЕ, ПРИБОРЫ, ПО И МАТЕРИАЛЫ

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

В качестве системной ОС в организации **LEFT** используется **Debian**

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

Вам доступен диск CentOS-7-x86_64-Everything-1804.iso

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

Вам доступен диск AdditionalPackages.iso, на котором располагаются недостающие RPMи deb пакеты

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 диаграммой.
2 Установите следующее ПО на ВСЕ виртуальные машины:
  2.1 Пакет tcpdump
  2.2 Пакет net-tools
  2.3 Редактор vim
  2.4 lynx
  2.5 bind-utils
  2.6 Клиент ftp
  2.7 Клиент lftp
3 На всех хостах сформируйте файл **/etc/hosts** в соответствии с Диаграммой (кроме адреса хоста L-CLI и R-CLI). Данный файл будет применяться во время проверки в случае недоступности DNS-сервисов. Проверка по IP-адресам выполняться не будет.
  3.1 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 сдиаграммой.
2 Настройте сервер протокола динамической конфигурации хостов для L-CLI.
  2.1 В качестве DHCP-сервера используйте L-FW.
    2.1.1 Используйте пул адресов 172.16.100.60 — 172.16.100.75.
    2.1.2 Используете адрес L-SRV в качестве адреса DNS-сервера.
  2.2 В качестве шлюза по умолчанию используйте соответствующий адрес L-FW.
  2.3 Используйте DNS-суффикс **skill39.wsr**
  2.4 DNS-записи типа A и PTR должны обновляться при получении адреса от DHCP-сервера.
3 На L-SRV настройте службу разрешения доменных имен.
  3.1 Сервер должен обслуживать зону **skill39.wsr**
  3.2 Сопоставление имен необходимо организовать в соответствии с Таблицей 1.
  3.3 Запросы, которые выходят за рамки зоны **skill39.wsr** должны пересылаться DNS-серверу ISP. Для проверки используйте доменное имя **worldskills.ru**.
  3.4 Реализуйте поддержку разрешения обратной зоны в соответствии с Таблицей 1.
  3.5 Файлы зон необходимо располагать в **/opt/dns/**
4 На DNS сервере ISP приобретена услуга Secondary DNS для зоны **skill39.wsr**
  4.1 Настройте возможность трансфера зоны **skill39.wsr** в сторону ISP.
  4.2 Используйте адрес ISP в качестве адреса DNS сервера для R-FW и R-CLI.
  4.3 Трансфер зоны на другие хосты, кроме ISP, должен быть запрещен.
5 На L-FW и R-FW настройте интернет-шлюз для организации коллективного доступа в Интернет.
  5.1 Настройте трансляцию сетевых адресов из внутренней сети в адрес внешнего интерфейса соответствующего межсетевого экрана.

Службы централизованного управления и журналирования

1 Разверните LDAP-сервер для организации централизованного управления учетными записями.
  1.1 В качестве сервера выступает L-SRV.
  1.2 Учетные записи создать в соответствии с Таблицей 2.
  1.3 Группы и пользователей создать в соответствии с Таблицей 2.
  1.4 Пользователи должны быть расположены в OU Users.
  1.5 Группы должны быть расположены в OU Groups.
  1.6 Хосты должны аутентифицироваться через LDAP в соответствии с Таблицей 2.
2 На L-SRV организуйте централизованный сбор журналов с хостов.
  2.1 Журналы должны храниться в директории **/opt/logs/**
  2.2 Журналирование должно производиться в соответствии с Таблицей 3.
  2.3 Сообщения в файлах журналов в директории **/opt/logs** не должны дублироваться.

Конфигурация служб удаленного доступа

1 Настройте сервер удаленного доступа на основе технологии OpenVPN:
  1.1 В качестве сервера выступает L-FW.
  1.2 Параметры туннеля
    1.2.1 Устройство TUN
    1.2.2 Протокол UDP
    1.2.3 Применяется сжатие
    1.2.4 Порт сервера 1122
  1.3 Ключевая информация должна быть сгенерирована на R-FW.
  1.4 В качестве адресного пространства подключаемых клиентов использовать сеть 5.5.5.0/27.
  1.5 Хранение всей необходимой (кроме конфигурационных файлов) информации организовать в **/opt/vpn**
2 На OUT-CLI настройте клиент удаленного доступа на основе технологии OpenVPN:
  2.1 Запуск удаленного подключения должен выполняться скриптом **start_vpn.sh**
  2.2 Отключение VPN-туннеля должно выполняться скриптом **stop_vpn.sh**
  2.3 Скрипты должны располагаться в **/opt/vpn**
  2.4 Скрипты должны вызываться из любого каталога без указания пути.
3 Настройте GRE-туннель между L-FW и R-FW:
  3.1 Используйте следующую адресацию внутри GRE-туннеля:
    3.1.1 L-FW: 10.5.5.1/30
    3.1.2 R-FW: 10.5.5.2/30
4 На L-FW настройте удаленный доступ по протоколу SSH:
  4.1 Доступ ограничен пользователями **ssh_p** и **ssh_c**
    4.1.1 В качестве пароля использовать **ssh_pass**
  4.2 SSH-сервер должен работать на порту **1022**.
5 На OUT-CLI настройте клиент удаленного доступа SSH:

5.1 Доступ к серверу L-FW должен происходить автоматически по правильному порту, без его явного указания номера порта в команде подключения.
5.2 Для других серверов по умолчанию должен использоваться порт **22**.
5.3 Доступ к L-FW под учетной записью **ssh_p** должен происходить с помощью аутентификации на основе открытых ключей.

Конфигурация веб служб

1 На R-FW установите и настройте веб-сервер:
1.1 Настройте веб-сайт для внешнего использования**www.skill39.wsr**
1.1.1 Используйте директорию **/var/www/html/out**
1.1.2 Используйте стандартные порты.
1.1.3 Обеспечьте работу сайта по протоколам **http** и **https** (сертификат должен быть сгенерирован на R-FW).
1.1.4 В случае доступности **https** должно происходить автоматическое перенаправление с **http**.
1.1.5 Клиенты должны доверять сертификату сайта.

Конфигурация служб хранения данных

1 Настройте сервер файлового хранилища на основе технологии NFS:
1.1 В качестве сервера должен выступать L-SRV.
1.2 В качестве хранилища используется каталог **/opt/nfs**
1.3 Доступ организуется для чтения и записи.
2 Настройте автоматическое монтирование NFS хранилища для клиентов L-CLI и R-CLI:
2.1 Используйте **/opt/nfs** в качестве пути для монтирования.
2.2 Клиенты L-CLI и R-CLI должны монтировать NFS каталог при запуске операционной системы.
3 Настройте FTP службу для доступа к файловому хранилищу:
3.1 В качестве сервера должен выступать L-SRV.
3.2 Корень FTP сервера должен располагаться в **/opt/nfs**
3.3 Обеспечьте доступ для клиента OUT-CLI с использованием стандартных портов протокола FTP по адресу **ftp.skill39.wsr**
3.4 Доступ должен быть ограничен пользователем **ftpuser:ftppass** с правами на чтение и запись.

Конфигурация параметров безопасности и служб аутентификации

1 Настройте CA на R-FW, используя OpenSSL.
1.1 Используйте **/etc/ca** в качестве корневой директории CA.
1.2 Атрибуты CA должны быть следующими:
1.2.1 Страна RU
1.2.2 Организация WorldSkillsRussia

1.2.3 CN должен быть установлен как WSR CA

1.3 Создайте корневой сертификат CA.

1.4 Все клиентские операционные системы должны доверять CA.

2 Настройте межсетевой экран **iptables** на L-FW и R-FW.

2.1 Запретите прямое попадание трафика из Интернет во внутренние сети.

2.2 Разрешите удаленные подключения с использованием OpenVPN на внешний интерфейс маршрутизатора L-FW.

2.3 Разрешите необходимый трафик для создания GRE туннеля между организациями.

2.4 Разрешите SSH подключения на соответствующий порт L-FW и R-FW.

2.5 Для VPN-клиентов должен быть предоставлен полный доступ к локальным сетям организаций LEFT и RIGHT.

2.6 Разрешите необходимый трафик к серверу L-SRV по транслированным IP-адресам.

2.7 Организуйте доступность сервиса DNS на L-SRV по внешнему адресу L-FW.

2.8 Разрешите необходимый трафик для работы веб и FTP служб.

2.9 Остальные сервисы следует запретить.

Таблица 1 – DNS-имена

Хост	**DNS-имя**
L-CLI	A,PTR: l-cli.skill39.wsr
L-SRV	A,PTR: l-srv.skill39.wsr CNAME: dns.skill39.wsr
L-FW	A: l-fw.skill39.wsr CNAME: vpn.skill39.wsr CNAME: ftp.skill39.wsr
R-FW	A: r-fw.skill39.wsr CNAME: www.skill39.wsr
R-CLI	A: r-cli.skill39.wsr

Таблица 2 – Учетные записи LDAP

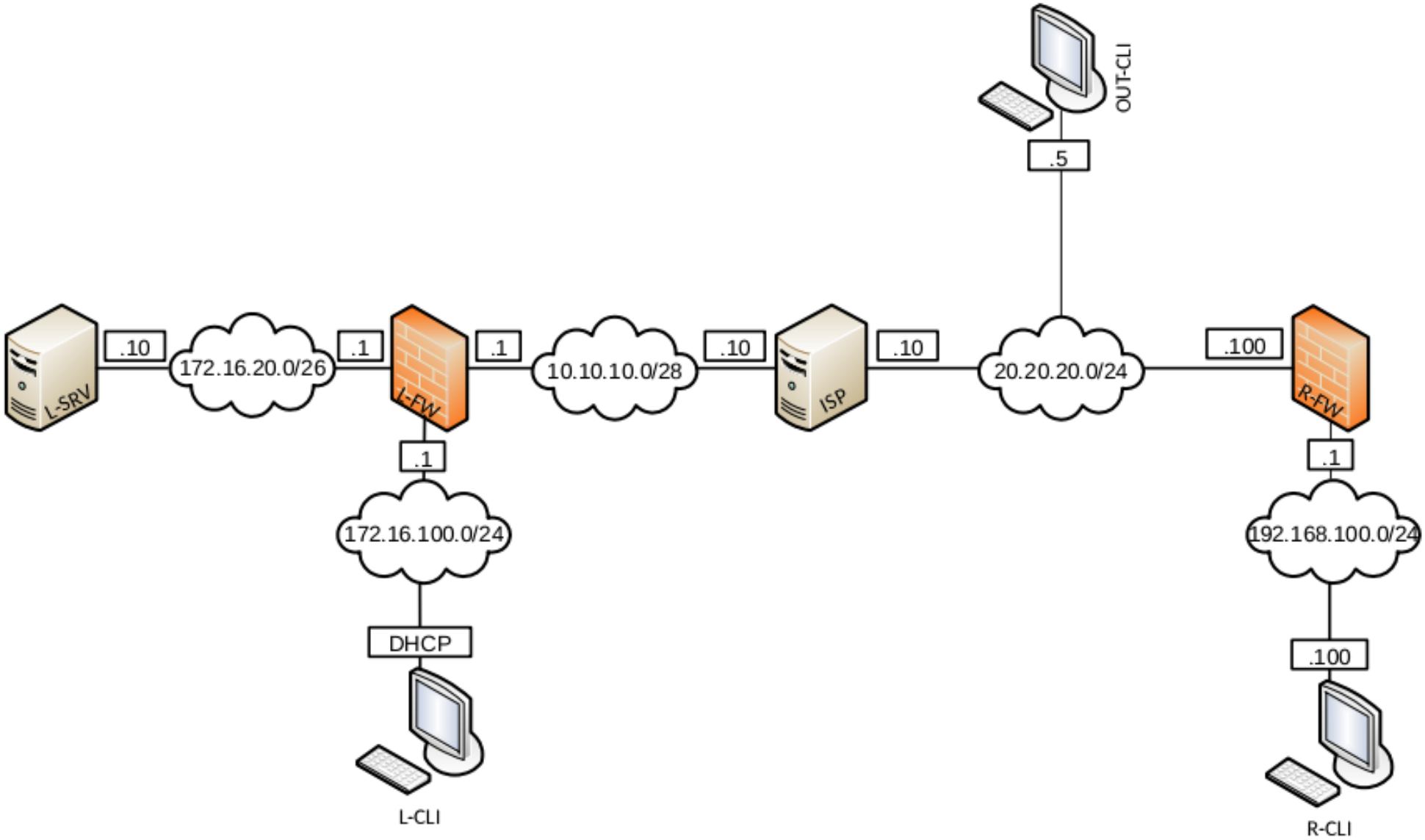
Группа	**CN**	**Пароль**	**Доступ**
Administrators	admin	toor	L-CLI L-FW
Users	user1 – user99	P@ssw0rd	L-CLI

Таблица 3 – Правила журналирования

Источник	**Уровень журнала**	**Файл**
L-SRV L-FW	critical	/opt/logs/<HOSTNAME>/crit.log
L-SRV	auth.*	/opt/logs/<HOSTNAME>/auth.log
L-FW	*.err	/opt/logs/<HOSTNAME>/error.log
L-CLI R-CLI	*.err	/opt/logs/err.log

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

ДИАГРАММА ВИРТУАЛЬНОЙ СЕТИ



Модуль B: «Пуско-наладка инфраструктуры на основе ОС семейства Windows»

Версия 1Б от 27.09.18.

ВВЕДЕНИЕ.

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

В рамках легенды конкурсного задания Вы – системный администратор компании, находящейся в Будапеште на восточном берегу Дуная. В главном офисе вы управляете доменом Pest.com. Вам необходимо настроить сервисы в локальной сети головного офиса.

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

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

Внимательно прочтите задание от начала до конца– оно представляет собой целостную систему. При первом доступе к операционным системам либо следуйте указаниям мастера, либо используйте следующие реквизиты: ***Administrator/P@ssw0rd*** *и* ***User/P@ssw0rd****– для клиентов.*

Если предоставленные виртуальные машины начнут самопроизвольно отключаться в процессе работы, попробуйте выполнить на них команду ***slmgr /rearm*** или обратитесь к техническому эксперту.

КОМПЛЕКТАЦИЯ КОНКУРСНОГО ЗАДАНИЯ

1 Текстовые файлы:
  1.1 данный файл с конкурсным заданием;
  1.2 файл дополнений к конкурсному заданию, содержащий: описание вида предустановок, описание используемых операционных систем,а также рекомендации по выделению ресурсов для виртуальных машин.
2 Предоставляемые конкурсантам компоненты проекта:
  2.1 файл для импорта пользователей в домен Pest.com (.xlsx);
  2.2 стартовая страница сайта managers.pest.com (.htm);
  2.3 стартовая страница сайта www.pest.com (.htm);
  2.4 стартовая страница сайта www.buda.pest.com (.htm).
3 Программное обеспечение:
  3.1 Windows Server 2016;
  3.2 Microsoft Office;
  3.3 RSAT tools for Windows 10;

3.4 Windows10.ADMX.

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

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

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

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

Настройка DC1

Базовая настройка

- переименуйте компьютер в DC1;
- перед установкой сетевых настроек решите задачу: вам дано адресное пространство следующего вида – «10.10.18.x/?». Длину маски рассчитайте исходя из того, чтобы в каждой образовавшейся подсети можно было разместить, ровно 14 клиентов. Для адресации в домене Pest.com используйте третью по счету подсеть; в качестве адреса DC1 используйте первый возможный адрес из этой подсети;
- обеспечьте работоспособность протокола ICMP (для использования команды ping).

ActiveDirectory

- сделайте сервер контроллером домена Pest.com.

DHCP

- настройтепротокол DHCP для автоконфигурации клиентов – в качестве диапазона выдаваемых адресов используйте все не занятые серверами адреса в подсети;
- настройте failover: mode – Loadbalancer, partner server – SRV1, state switchover – 10 min;
- настройте дополнительные свойства области (адреса DNS-серверов и основного шлюза).

DNS

- настройте необходимые зоны прямого и обратного просмотра;
- создайте вручную все необходимые записи типа A и PTR для серверов домена инеобходимых web-сервисов.

GPO

- запретите анимацию при первом входе пользователей в систему на всех клиентских компьютерах домена;
- члены группы IT должны быть членами группы локальных администраторов на всех клиентских компьютерах домена;
- в браузерах IEExplorer и MicrosoftEdge (установите и используйте windows10.admx) должна быть настроена стартовая страница – www.Pest.com;
- для членов группы Experts настройте перенаправление папок *myDocuments* и *Desktop* по адресу SRV1→d:\shares\redirected.

Элементы доменной инфраструктуры

- создайте подразделения: Experts, Competitors, Managers, Visitors и IT;
- всоответствующихподразделенияхсоздайтедоменныегруппы: Experts, Competitors, Managers, Visitors, IT;

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 ActiveDirectory); 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 SRV1→d:\shares\users;
- все пользователи при первом входе в домен с компьютера CLI1 должны видеть на рабочем столе ярлык программы *Калькулятор*.

Настройка SRV1

Базовая настройка

- переименуйте компьютер в SRV1;
- перед установкой сетевых настроек решите задачу: вам дано адресное пространство следующего вида – «10.10.18.x/?». Длину маски рассчитайте исходя из того, чтобы в каждой образовавшейся подсети можно было разместить, ровно 14 клиентов. Для адресации в домене Pest.com используйте третью по счету подсеть; в качестве адреса SRV1 используйте второй возможный адрес из этой подсети;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к домену Pest.com;
- с помощью дополнительных жестких дисков создайте зеркальныймассив; назначьте ему букву D:\.

Active Directory

- сделайте сервер дополнительным контроллером домена Pest.com.

DHCP

- настройте протокол DHCP для автоконфигурации клиентов;
- настройте failover: mode – Loadbalancer, partner server – DC1, state switchover – 10 min;

DNS

- сделайте сервер дополнительным DNS-сервером в домене Pest.com;
- загрузите с DC1 все зоны прямого и обратного просмотра.

Общие папки

- создайте общие папки для подразделений (Competitors, ExpertsandManagers) по адресу SRV1→d:\shares\departments;
- обеспечьте привязку общей папки подразделения к соответствующей группе в качестве диска G:\.

Квоты/Файловые экраны

- установите максимальный размер в 1Gb 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 для менеджеров компании (используйте предоставленный htm-файл в качестве документа по умолчанию);
- сайт должен быть доступен по имени managers.pest.com;
- в будущем администраторы будут выкладывать на сайт важные новости, которые ни в коем случае не должны пропасть – предусмотрите возможность автоматического сохранения всего содержимого сайта на сервер DC1 (место и способ хранения укажите в сопроводительной документации).

Настройка CLI1

Базовая настройка

- переименуйте компьютер в CLI1;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к домену Pest.com;
- установите набор компонентов удаленного администрирования RSAT;
- запретите использование «спящего режима» таким образом, чтобы пользователи домена не могли изменить эту настройку без участия администратора домена;
- используйте компьютер для тестирования настроек в домене Pest.com: пользователей, общих папок, групповых политик, в том числе – тестирования удаленных подключений через DirectAccess (временно переключая компьютер в сеть Internet).

Настройка DC2

Базовая настройка

- переименуйте компьютер в DC2;
- перед установкой сетевых настроек решите задачу: вам дано адресное пространство следующего вида – «192.168.19.y/?». Длину маски рассчитайте исходя из того, чтобы в

данном пространстве имелось, ровно 8 подсетей. Для адресации в поддомене Buda.Pest.com используйте вторую по счету подсеть; в качестве адреса DC2 используйте первый возможный адрес из этой подсети;
- обеспечьте работоспособность протокола ICMP (для использования команды ping).

ActiveDirectory
- сделайте сервер контроллером поддомена Buda.Pest.com.

DHCP
- настройте протокол DHCP для автоконфигурации клиентов – в качестве диапазона выдаваемых адресов используйте все не занятые серверами адреса в подсети.

DNS
- настройте необходимые зоны прямого и обратного просмотра;
- создайте вручную все необходимые записи типа A и PTR для серверов домена и необходимых web-сервисов;
- обеспечьте разрешение имен сайтов www.pest.com и www.buda.pest.com (оба сайта должны быть доступны со всех клиентских компьютеров сети предприятия).

Элементы доменной инфраструктуры
- для всех пользовательских учетных записей в поддомене используйте перемещаемые профили;
- для хранения профилей пользователей используйте общую папку по адресу DC2 →c:\profiles;
- каждый пользователь должен иметь доступ только к файлам своего профиля; при обращении к указанной общей папке средствами программы *Проводник* пользователь должен видеть в списке только папку со своим профилем.

IIS
- создайте сайт www.pest.com (используйте предоставленный htm-файл в качестве документа по умолчанию);
- создайте сайт www.buda.pest.com (используйте предоставленный htm-файл в качестве документа по умолчанию);

Настройка CLI2

Базовая настройка
- переименуйте компьютер в CLI2;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к поддомену Buda.Pest.com;

- запретите использование «спящего режима» таким образом, чтобы пользователи поддомена не могли изменить эту настройку без участия администратора поддомена;
- используйте компьютер для тестирования настроек в поддомене Buda.Pest.com.

Настройка BRIDGE2

Базовая настройка

- переименуйте компьютер в BRIDGE2;
- задайте настройки сети следующим образом: для сетевого интерфейса, подключенного к ISP, используйте адрес 200.100.100.5/24; для сетевого адреса в подсети Buda.pest.com используйте последний возможный адрес из рассчитанной ранее подсети;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к поддомену Buda.Pest.com.

Настройка RRAS

- установите службу RRAS;
- настройте VPN-соединение с доменом Pest.com по протоколу PPTP; весь трафик между доменами должен передаваться через это соединение.

Настройка BRIDGE1

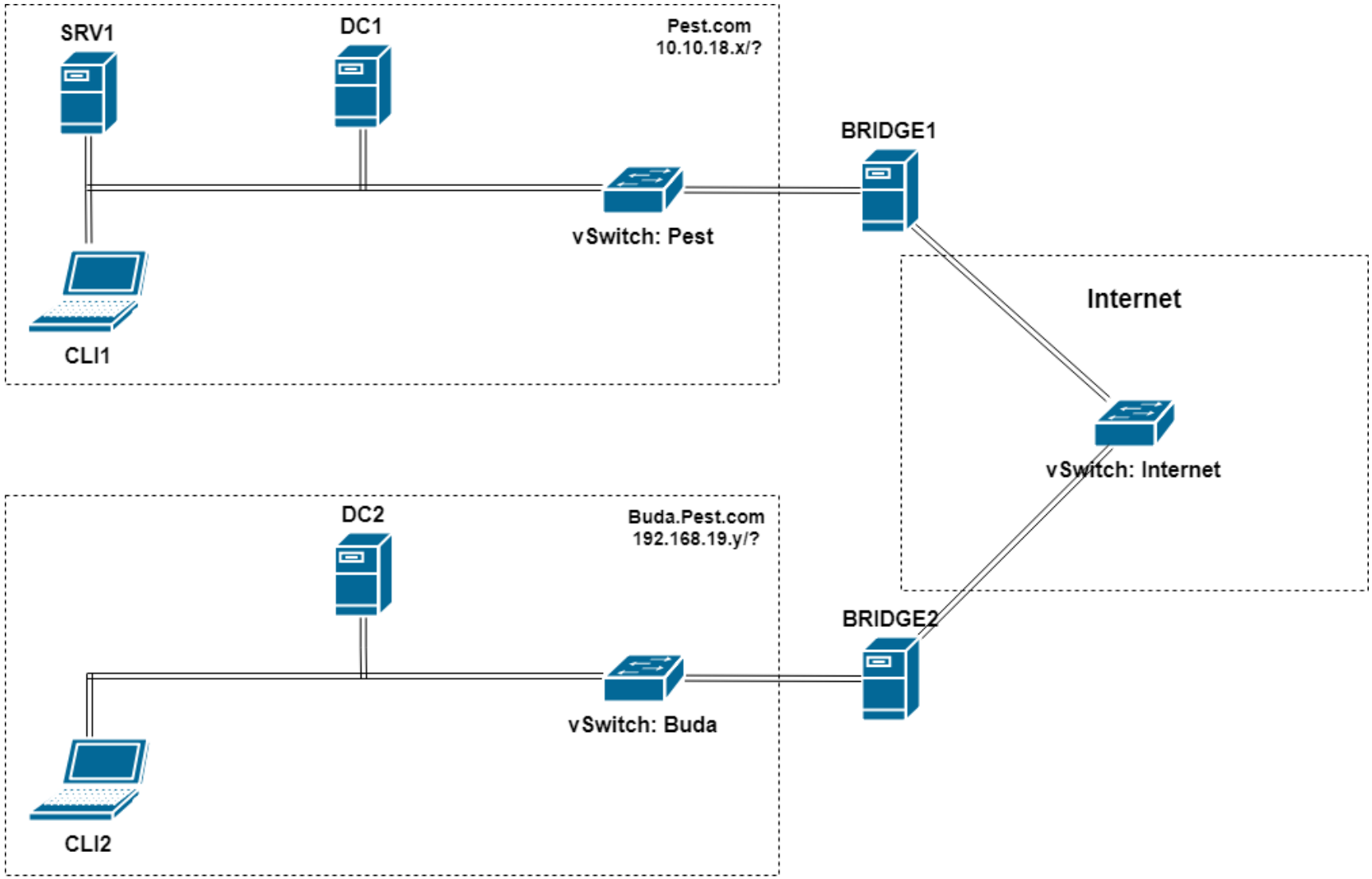
Базовая настройка

- переименуйте компьютер в BRIDGE1;
- задайте настройки сети следующим образом: для сетевого интерфейса, подключенного к ISP, используйте адрес 200.100.100.1/24; для сетевого адреса в подсети pest.com используйте последний возможный адрес из рассчитанной ранее подсети;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к домену Pest.com.

Настройка RRAS

- установите службу RRAS;
- настройте защищенное VPN-соединение с поддоменом Buda.pest.com по протоколу PPTP; весь трафик между доменами должен передаваться через это соединение.

ДИАГРАММА ВИРТУАЛЬНОЙ СЕТИ



Модуль С: «Пуско-наладка телекоммуникационного оборудования»

Версия 1Б от 27.09.18.

ВВЕДЕНИЕ

Знание сетевых технологий на сегодняшний день становится незаменимым для тех, кто хочет построить успешную карьеру в области ИТ. Данное конкурсное задание содержит множество задач, основанных на опыте реальной эксплуатации информационных систем, в основном интеграции и аутсорсинге. Если вы можете выполнить задание с высоким результатом, то вы точно сможете обслуживать информационную инфраструктуру большого предприятия.

ОПИСАНИЕ КОНКУРСНОГО ЗАДАНИЯ

Данное конкурсное задание разработано с учетом различных сетевых технологий, соответствующих уровням сертификации CCNA R\S Задание разбито на следующие секции:

- Базовая настройка
- Настройка коммутации
- Настройка подключений к глобальным сетям
- Настройка маршрутизации
- Настройка служб
- Настройка механизмов безопасности
- Настройка параметров мониторинга и резервного копирования
- Конфигурация виртуальных частных сетей

Все секции являются независимыми друг от друга, но вместе образуют достаточно сложную сетевую инфраструктуру. Некоторые задания достаточно просты и понятны, некоторые могут быть неочевидными. Можно заметить, что некоторые технологии должны работать в связке или поверх других технологий. Например, может подразумеваться, что IPv6 маршрутизация должна работать поверх настроенной виртуальной частной сети, которая, в свою очередь, должна работать поверх IPv4 маршрутизации, которая, в свою очередь, должна работать поверх PPPoE и FrameRelay и т.д. Очень важно понимать, что если вам не удается решить какую-либо из задач по середине такого технологического стека, это не значит, что решенные задачи не будут оценены. Например, если вы не можете настроить динамическую маршрутизацию IPv4, которая необходима для работы виртуальной частной сети, вы можете использовать статическую маршрутизацию и продолжать работу над настройкой виртуальной частной сети и всем что должно работать поверх нее. В этом случае вы не получите баллы за динамическую маршрутизацию, но вы получите баллы за всё что должно работать поверх нее (в случае если функциональные тесты пройдены успешно).

ИНСТРУКЦИИ ДЛЯ УЧАСТНИКА

В первую очередь необходимо прочитать задание полностью и составить алгоритм выполнения работы. Вам предстоит вносить изменения в действующую, преднастроенную

сетевую инфраструктуру предприятия, состоящую из головного офиса HQ и удаленного офиса BR1. Офисы имеют связь через провайдера ISP1. 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 и BR1.

У вас отсутствует консольный доступ к устройствам, будьте очень внимательны при выполнении задания! В случае потери связи с оборудованием, вы будете виноваты сами. Разрешается перезагрузка оборудования – только техническими экспертами. Например, применили неправильный ACL, который закрыл доступ по telnet, но вы не успели сохранить конфигурацию.

Руководствуйтесь пословицей: Семь раз отмерь, один раз отрежь. Для выполнения задания у вас есть одна физическая машина(PC1 с доступом по Telnet), которую вы должны использовать в качестве:

PC1 ПК, Windows7, Putty, tftpd32. Пользователь User пароль P@ssw0rd. Компьютер используется для соединения в сетях Office и BR3

SRV1 ПК, Debian пользователь **root**пароль **toor**, с предустановленными сервисами

1) SNMP – для проверки используется пакет **net-snmp-utils,** используйте команду **snmp_test_HQ**

2) NTP- реализован демоном **chrony**

3) TFTP папка для проверки **/Cisco_TFTP** реализован пакетом **xinetd**

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 всем сетевым устройствам используйте пароль: **cisco** и пароль для привилегированного режима: **cisco**

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

SW1 – 192.168.254.10

SW2 – 192.168.254.20

SW3 – 192.168.254.30

HQ1 – 192.168.254.1

Для подключения к устройствам в удаленном офисе BR1, подключите рабочую станцию в порт Fe0/1 маршрутизатора BR1. BR1 доступен по адресу 192.168.1.1.

Базовая настройка

1 Задайте имя всех устройств в соответствии с топологией.
2 Назначьте для всех устройств доменное имя **wsr2018.ru**.
3 Создайте на всех устройствах пользователей **wsr2018** с паролем **cisco**
  3.1 Пароль пользователя должен храниться в конфигурации в виде результата хэш-функции.
  3.2 Пользователь должен обладать максимальным уровнем привилегий.
4 На всех устройствах установите пароль **wsr** на вход в привилегированный режим.
  4.1 Пароль должен храниться в конфигурации НЕ в виде результата хэш-функции.
5 Настройте режим, при котором все пароли в конфигурации хранятся в зашифрованном виде.
6 Для всех устройств реализуйте модель AAA.
  6.1 Аутентификация на линиях виртуальных терминалов с 0 по 15 должна производиться с использованием локальной базы учётных записей. После успешной аутентификации при удалённом подключении пользователи сразу должен получать права, соответствующие их уровню привилегий или роли.
  6.2 Настройте необходимость аутентификации на локальной консоли.
  6.3 При успешной аутентификации на локальной консоли пользователи должны сразуполучать права, соответствующие их уровню привилегий или роли.
7 На устройствах, к которым разрешен доступ, в соответствии с топологиями L2 и L3, создайте виртуальные интерфейсы, под интерфейсы и интерфейсы типа петля, назначьте IP-адреса.
8 Все устройства должны быть доступны для управления по протоколу SSH версии **2**.

Настройка коммутации

1 Для централизованного конфигурирования VLAN в коммутируемой сети предприятия используйте протокол VTP версии **3**.
  1.1 В качестве основного сервера VTP настройте SW1.
  1.2 Коммутаторы SW2 и SW3 настройте в качестве VTP клиента.
  1.3 В качестве домена используйте **wsr2018.ru**
  1.4 Используйте пароль **VTPPass** для защиты VTP.
  1.5 Таблица VLAN должна содержать следующие сети:
    1.5.1 VLAN100 с именем MGT.
    1.5.2 VLAN200 с именем DATA.
    1.5.3 VLAN300 с именем OFFICE.
    1.5.4 VLAN400 с именем KTK
2 Между всеми коммутаторами настройте транки с использованием протокола IEEE 802.1q.
  2.1 Порты F0/10 коммутаторов SW1 и SW3, должны быть работать в режиме доступа без использования согласования. Отключите протокол DTP явным образом.
  2.2 Транк между коммутаторами SW2 и SW3 должен быть настроен без использования согласования. Отключите протокол DTP явным образом.
  2.3 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.

3 Настройте агрегирование каналов связи между коммутаторами.
   3.1 Номера портовых групп:
      1 – между коммутаторами SW1 (F0/1-3) и SW2 (F0/1-3);
      2– между коммутаторами SW2 (F0/6-7) и SW3 (F0/6-7);
   3.2 Агрегированный канал между SW1 и SW2 должен быть организован с использованием протокола согласования LACP. SW1 должен быть настроен в активном режиме, SW2 в пассивном.
   3.3 Агрегированный канал между SW2 и SW3 должен быть организован с использованием протокола согласования PAgP. SW2 должен быть настроен в предпочтительном, SW3 в автоматическом.
4 Конфигурация протокола остовного дерева:
   4.1 Используйте протокол Rapid STP.
   4.2 Коммутатор SW1 должен являться корнем связующего дерева в сетях VLAN 100, 200 и 300, в случае отказа SW1, корнем должен стать коммутатор SW2.
   4.3 Настройте используемые порты коммутаторов SW1 и SW2 так, чтобы во всех VLAN корнем связующего дерева могли стать только SW1 или SW2, а при получении BPDU пакета с лучшим приоритетом корня, порт должен перейти в состояние root-inconsistent.
   4.4 Настройте порт F0/10 коммутатора SW2, таким образом, что при включении они сразу переходили в состояние forwarding не дожидаясь пересчета остовного дерева. При получении BPDU пакета данные порты должны переходить в состояние error-disabled.
5 Настройте порты F0/10 коммутаторов SW1 и SW2, в соответствии с L2 диаграммой. Порты должны быть настроены в режиме доступа.
6 Настройте порт F0/24 коммутатора SW1 в соответствии с L2 диаграммой.
7 Отключите протокол CDP на маршрутизаторах HQ1 и BR1, только на портах в сторону провайдера ISP1.

Настройка подключений к глобальнымсетям

1 Настройте подключение PPPoE между ISP1 и маршрутизатором BR1.
   1.1 Настройте PPPoE клиент на BR1.
   1.2 Используйте имя пользователя **cisco** и пароль **cisco**
   1.3 Устройства походят **одностороннюю** аутентификацию по протоколу **CHAP**, только ISP1 проверяет имя пользователя и пароль.
   1.4 BR1 должен автоматически получать адрес от ISP1.
2 Настройте подключение HQ1 к провайдеру ISP1 с помощью протокола PPP.
   2.1 Не используйте аутентификацию.
   2.2 HQ1 должен автоматически получать адрес от ISP1.

Настройка маршрутизации

1 Настройте протокол динамической маршрутизации OSPF в офисе BR1 с главным офисом HQ.
   1.1 Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
   1.2 Используйте магистральную область для GRE туннеля.

1.3 Соседства между офисами HQ и BR1 должны устанавливаться через защищенный туннель.
1.4 В офисе BR1 используйте область с номером 1.
1.5 Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.

2 ISP1 предоставляет подсеть PA (ProviderAggregatable) адресов (11.11.11.11/32) для офиса BR1. На маршрутизаторе BR1 настройте протокол динамической маршрутизации EIGRP с номером автономной системы **2018**.
2.1 Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
2.2 Используйте аутентификацию MD5 с помощью связки ключей EIGRPс ключом **WSR** и номером ключа **2**.
2.3 Провайдер ISP1 выполняет редистрибуцию маршрута 11.11.11.11/32 в сеть BGP, убедитесь в том, что вы корректно анонсируете данный маршрут провайдеру.

3 Офис HQ имеет подсети PI (ProviderIndependent) адресов и автономную систему 65000. На маршрутизаторе настройте протокол динамической маршрутизации BGP в соответствии с таблицей

Устройство	AS
HQ1	65000
ISP1	65001

3.1 Настройте автономные системы в соответствии с Routing-диаграммой.
3.2 Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.

4 Настройте прокол динамической маршрутизации OSPFv3 поверх защищенного туннеля. На маршрутизаторах HQ1 и BR1 настройте протокол динамической маршрутизации OSPFv3 с номером процесса 1.
4.1 Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
4.2 Используйте зону с номером **0**.
4.3 Настройте аутентификацию MD5 для магистральной зоны.

Настройка служб

1 В сетевой инфраструктуре сервером синхронизации времени является SRV1. Все остальные сетевые устройства должны использовать в качестве сервера времени HQ1.
1.1 Передача данных между HQ1 и SRV1 осуществляется без аутентификации.
1.2 Настройте временную зону с названием MSK, укажите разницу с **UTC +3** часов.
1.3 Настройте сервер синхронизации времени. Используйте стратум **2**.
1.4 Используйте для синхронизациклиентов с HQ1 аутентификацию MD5 с ключом **WSR**.

2 Настройте динамическую трансляцию портов (PAT):
2.1 На маршрутизаторе BR1 настройте динамическую трансляцию портов (PAT) для сети 192.168.1.0/24 в адрес петлевого интерфейса 11.11.11.11.

3 Настройте протокол динамической конфигурации хостов со следующими характеристиками
3.1 На маршрутизаторе HQ1 для подсети OFFICE:
3.2 Адрес сети – 30.30.30.0/24.
3.3 Адрес шлюза по умолчанию интерфейс роутера HQ1.

3.4 Адрес TFTP-сервера 172.16.20.2.
3.5 Компьютер PC1 должен получать адрес 30.30.30.30.

Настройка механизмов безопасности

1 На маршрутизаторе BR1 настройте пользователей с ограниченными правами.
1.1 Создайте пользователей **user1** и **user2** с паролем **cisco**
1.2 Назначьте пользователю **user1** уровень привилегий **5**. Пользователь должен иметь возможность выполнять все команды пользовательского режима, а также выполнять перезагрузку и отладку с помощью команд debug.
1.3 Создайте и назначьте view-контекст sh_view на пользователя
1.3.1 Команду show cdp neighbor
1.3.2 Все команды showip *
1.3.3 Команду who
1.4 Создайте view-контекст ping_view. Включите в него
1.4.1 Команду ping
1.4.2 Команду traceroute
1.5 Создайте superview-контекстс именем super, объединяющий эти 2 контекста. При входе на маршрутизатор пользователь user2 должен попадать в данный контекст
1.6 Убедитесь, что пользователи не могут выполнять другие команды в рамках присвоенных контекстов и уровней привилегий.
2 На порту F0/10 коммутатора SW3, включите и настройте PortSecurity со следующими параметрами:
2.1 не более 2 адресов на интерфейсе
2.2 адреса должны динамически определяться, но не сохраняться в конфигурации.
2.3 при попытке подключения устройства с адресом, нарушающим политику, на консоль должно быть выведено уведомление, порт не должен быть отключен.
3 На коммутаторе SW3 включите DHCP Snooping для подсети OFFICE. Используйте флеш-память в качестве места хранения базы данных.
4 На коммутаторе SW3 включите динамическую проверку ARP-запросов в сети OFFICE. Сделайте порт Fa0/11 доверенным.

Настройка параметров мониторинга и резервного копирования

1 На маршрутизаторе HQ1 и BR1 настройте возможность удаленного мониторинга по протоколу SNMP v3.
1.1 Задайте местоположение устройств MSK, Russia
1.2 Задайте контакт admin@wsr.ru
1.3 Используйте имя группы WSR.
1.4 Создайте профиль только для чтения с именем RO.
1.5 Используйте для защиты SNMP шифрование AES128 и аутентификацию SHA1.
1.6 Используйте имя пользователя: **snmpuser** и пароль: **snmppass**
1.7 Для проверки вы можете использовать команду snmp_test_HQна SRV1.
2 На маршрутизаторе HQ1 настройте резервное копирование конфигурации

2.1 Резервная копия конфигурации должна сохраняться на клиент по протоколу TFTP при каждом сохранении конфигурации в памяти устройства

2.2 Для названия файла резервной копии используйте шаблон <hostname><time>.cfg

Конфигурация виртуальных частныхсетей

1 На маршрутизаторах HQ1и BR1 настройте DMVPN:

1.1 Используйте в качестве VTI интерфейс Tunnel1

1.2 Используйте адресацию в соответствии с L3-диаграммой

1.3 Режим — GRE

1.4 Интерфейс-источник — Loopback-интерфейс на каждом маршрутизаторе.

2 Защита туннеля должна обеспечиваться с помощью IPsec.

2.1 Параметры политики первой фазы:

2.1.1 Проверка целостности – SHA-384

2.1.2 Шифрование – AES-192

2.1.3 Группа Диффи-Хэлмана – 14

2.1.4 Используйте аутентификацию по ключу **wsr**.

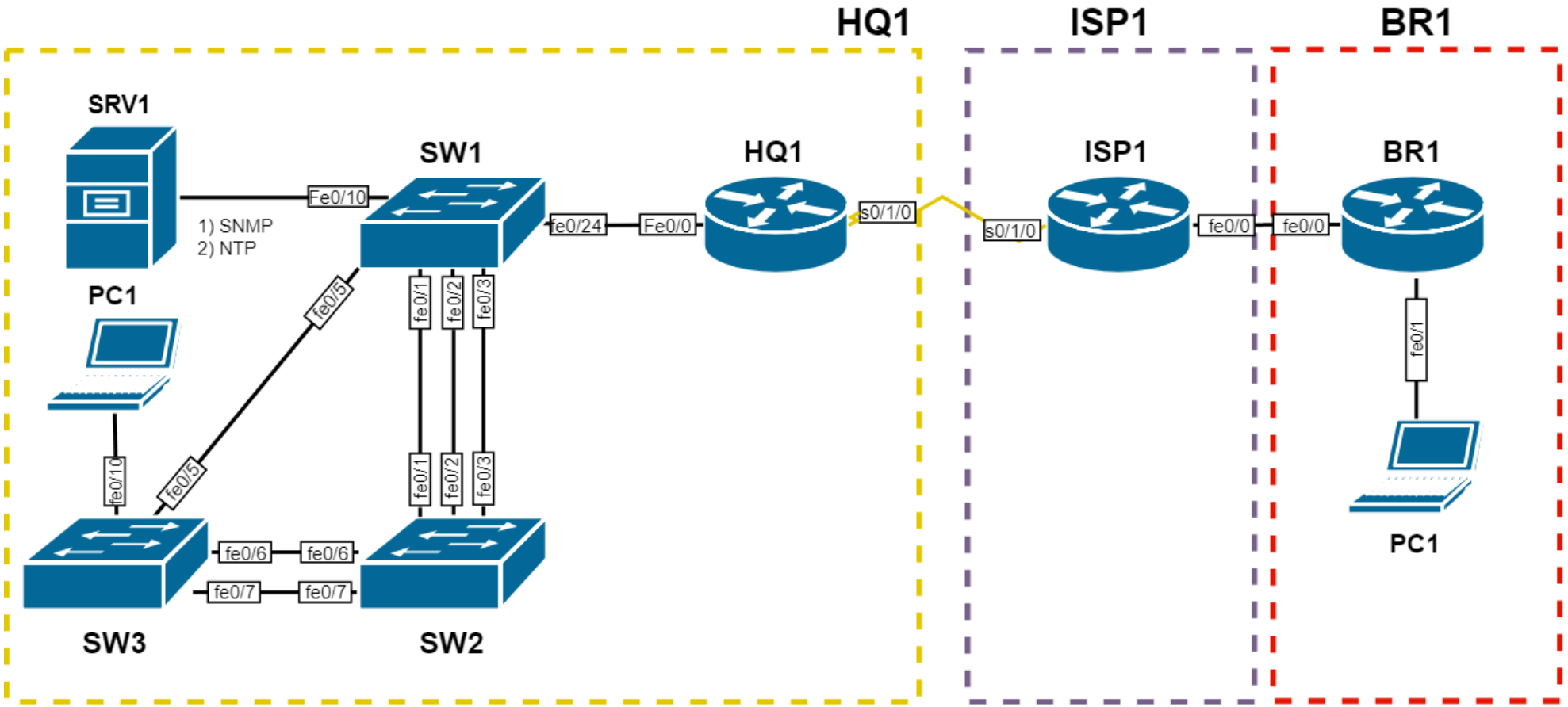
2.2 Параметры преобразования трафика для второй фазы:

2.2.1 Протокол – ESP

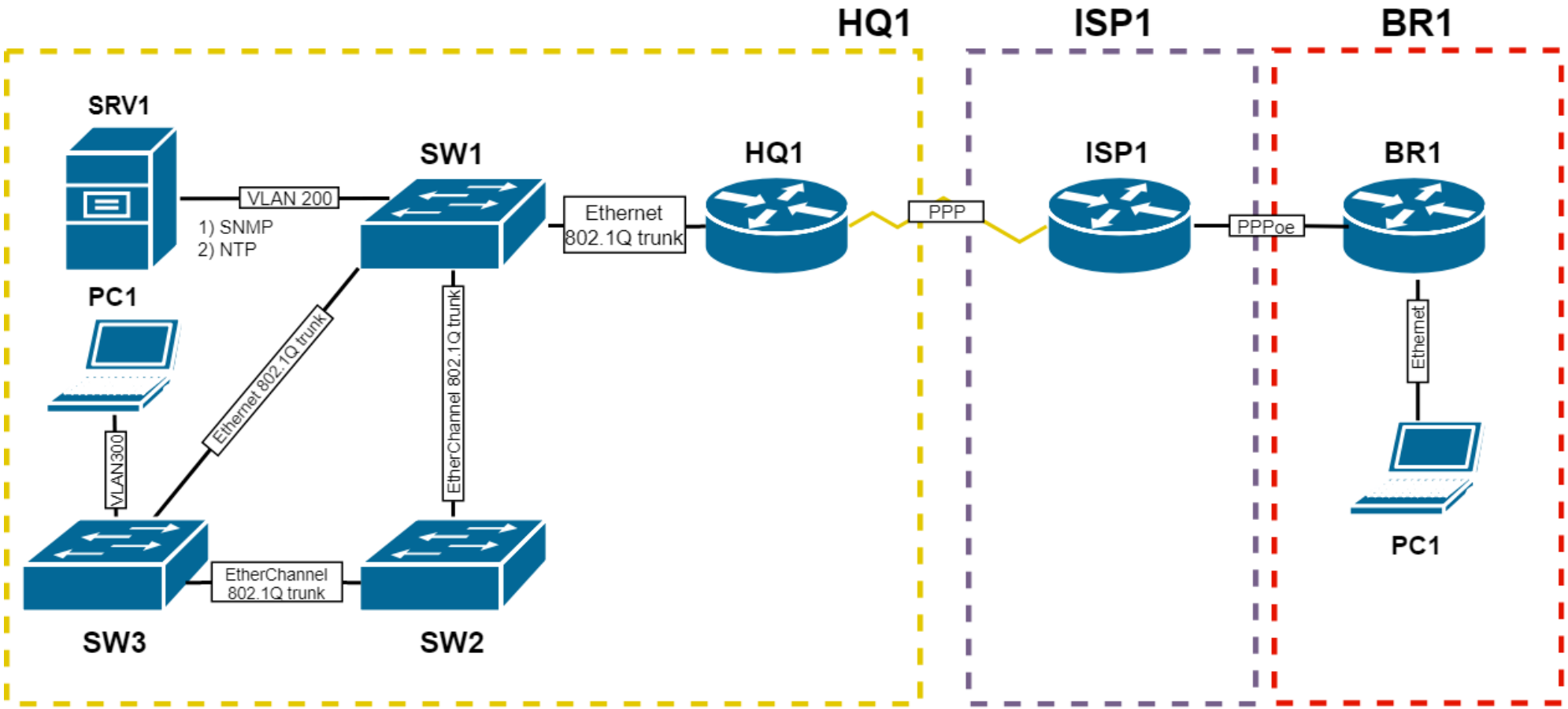
2.2.2 Шифрование – AES

2.2.3 Проверка целостности – MD5

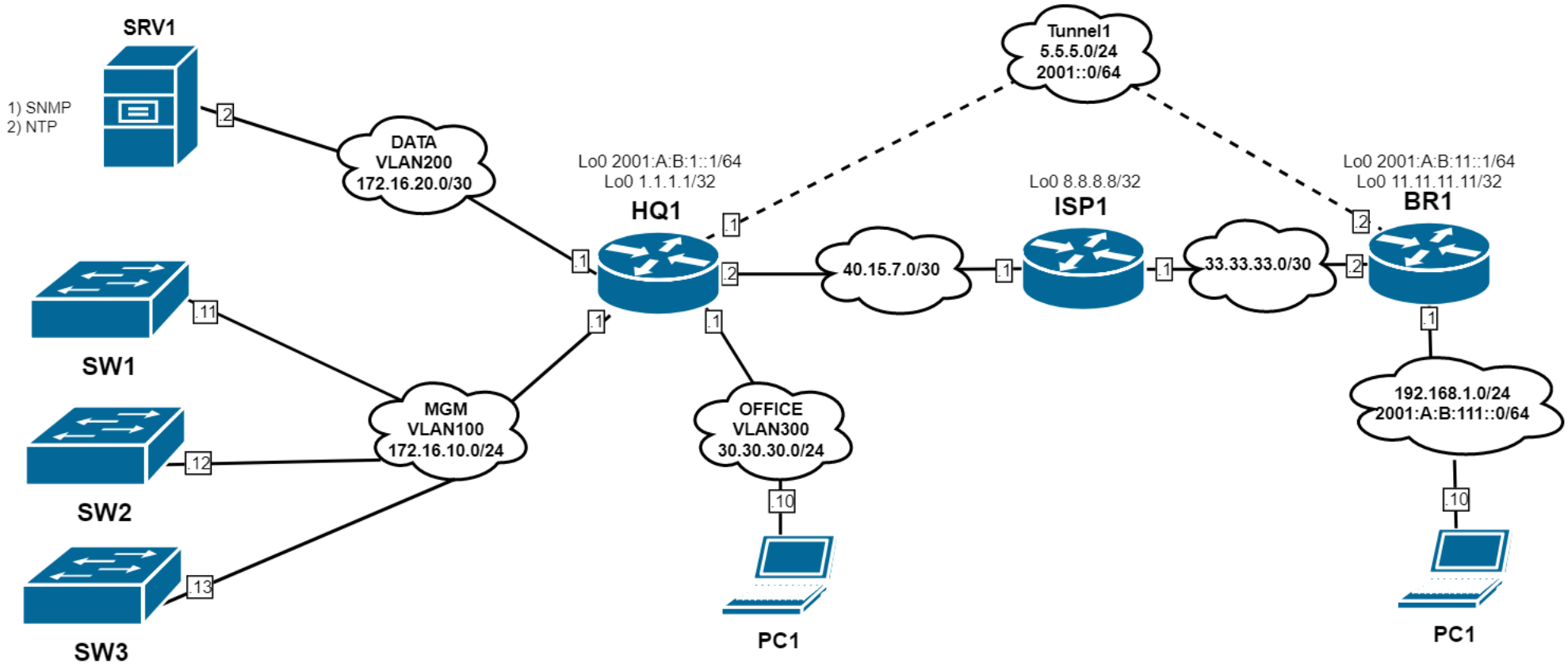
Топология L1



Топология L2



Топология L3



Routing-диаграмма