Конкурсное задание

КОМПЕТЕНЦИЯ «СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

Конкурсное задание включает в себя следующие разделы:

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

Количество часов на выполнение задания: 10 ч.

1. ФОРМЫ УЧАСТИЯ В КОНКУРСЕ

Индивидуальный конкурс.

2. ЗАДАНИЕ ДЛЯ КОНКУРСА

Содержанием конкурсного задания являются работы по пуско-наладке сетевой инфраструктуры на базе современного сетевого оборудования и операционных систем семейства Windows и Linux. Участники соревнований получают инструкцию, сетевые диаграммы и методические рекомендации по выполнению. Конкурсное задание является комплексным и выполняется как единое целое с точкой STOP.

Задание чемпионата 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 ОС семейства Linux; Пуско-наладку инфраструктуры на основе ОС семейства Windows; Пуско-наладку телекоммуникационного оборудования.

Окончательная методика проверки уточняются членами жюри. Оценка производится в отношении работы модулей. Если участники конкурса не выполняют требования техники безопасности, подвергают 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 как единое задание со стоп точками. Оценка происходит Ежедневно.

Задания разработаны и протестированы группой сертифицированных экспертов:

Модуль конкурсного задания	Роль	ФИО Эксперта
Конкурсное задание	Ведущий разработчик	А.А. Щербинин
	Группа разработки	Н.О. Силаев
	Группа разработки	Д.В. Дюгуров

3. МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ

Модули и время приведены в таблице 1

Таблица 1 – Время выполнение модуля

№ п/п	Наименование модуля	Рабочее время	Время на задание
1	Конкурсное задание день 1	10	5 ч.
2	Конкурсное задание день 2		5 ч.

Конкурсное задание

Версия 1.0.1 от 26.02.2019

ВВЕДЕНИЕ

Данное конкурсное задание содержит множество задач, основанных на опыте реальной эксплуатации информационных систем в сфере интеграции и аутсорсинга корпоративных вычислительных сетей. Если вы можете выполнить задание с высоким результатом, то вы сможете достаточно успешно обслуживать информационную инфраструктуру большого предприятия, ну, или хотя бы делать вид.

ОПИСАНИЕ КОНКУРСНОГО ЗАДАНИЯ

Данное конкурсное задание разработано с использованием различных технологий, входящих в сертификационные программы LPIC, Red Hat, CCNA, CCNP, MCSA.

Совместное использование этих технологий представляет собой достаточно сложную инфраструктуру. Требования в задании представлены в общем виде, конкретный метод выполнения и технологии, необходимые для его реализации, вы вправе выбрать самостоятельно с учётом указанных в задании требований.

Можно заметить, что многие технологии должны работать в связке или поверх других. Например, динамическая маршрутизация должна выполняться поверх настроенного между организациями туннеля. Важно понимать, что если вам не удалось настроить полностью технологический стек, то это не означает что работа не будет оценена. Например, для удаленного доступа необходимо настроить IPsec-туннель, внутри которого организовать GRE-туннель. Если вам не удалось настроить IPsec, но вы смогли настроить GRE, то вы все еще получите баллы за организацию удаленного доступа.

Главной задачей является получение работоспособной системы в том или ином виде, а также её ежедневная доработка и улучшение.

СХЕМА ОЦЕНКИ

Оцениваемые аспекты имеют разный вес в зависимости от их сложности. Схема оценки построена так, чтобы каждый аспект оценивался только один раз. Например, в задании предписывается настроить корректные имена для всех устройств, данный аспект будет оценен в первый день только один раз и повторная оценка данного аспекта проводится не будет. 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.

Следует также учесть, что для данного задания предусмотрена автоматическая оценка результатов.

Процедура оценки результатов выполнения задания будет производиться в конце каждого конкурсного дня, причем оцениваться будут именно те технологии, работоспособность которых ожидается по окончании текущего конкурсного дня. Участники могут выполнять задачи «на будущее», но им следует быть уверенными, что при этом не нарушается работоспособность технологий текущего конкурсного дня. Например, в первый день необходимо настроить веб-сервер, работающий по протоколу HTTP, а в третий день включить перенаправление на HTTPS. Если участники включат перенаправление на HTTPS в первый день, то они, скорее всего, могут не получить баллов за работу протокола HTTP в конце первого дня.

Проверка будет производиться с использованием доменных имен. Проверка по IP-адресам выполняться не будет.

НЕОБХОДИМОЕ ОБОРУДОВАНИЕ, ПРИБОРЫ, ПО И МАТЕРИАЛЫ

Конкурсное задание выполнимо в полном объеме с привлечением оборудования и материалов, указанных в Инфраструктурном листе.

ПРЕДНАСТРОЙКИ РАБОЧЕГО МЕСТА

1) На всех узлах под управлением ОС Linux установлены пакеты программного обеспечения.
    a) Пакет tcpdump.
    b) Пакет net-tools.
    c) Браузер lynx.
    d) Пакет dns-utils.
    e) Клиент ftp.
    f) Клиент lftp.
    g) Пакет sshpass.
    h) Пакет curl.
    i) Пакет open-vm-tools.
2) На всех предустановленных Windows-машинах установлены гостевые дополнения VMWare, а также выполнена команда *sysprep*.
3) Ряд дополнительных пакетов и приложений, а также комплекты документации доступны на сервере Moogle.ru, имитирующем реальную работу сети Интернет.
4) Все сетевые устройства сконфигурированы для удалённого администрирования из соответствующих локальных сетей по протоколу Telnet. На межсетевой экран скопированы дистрибутив ASDM и образ клиента AnyConnect.
5) Параметры интернет-провайдеров, предоставляющих услуги организации или клиентам.
    a) GOSTELECOM
        i) Адрес IPv4/Маска: 77.34.141.141/22
        ii) Шлюз: 77.34.140.1
        iii) Адрес IPv6/Маска: 2a01:620::2018/64
        iv) Шлюз: 2a01:620::1
        v) Делегируемый префикс: 2a01:620:1337::/48
        vi) AS: 12332
    b) GIGAFON
        i) Адрес IPv4/Маска: 178.207.179.6/29
        ii) Шлюз: 178.207.179.1
        iii) Адрес IPv6/Маска: 2a03:d000:2000::2000/64
        iv) Шлюз: 2a03:d000:2000::1
        v) Делегируемый префикс: 2a03:d000:2001::/48
        vi) AS: 31133
    c) TTL
        i) Адрес IPv4/Маска: 62.33.111.111/25
        ii) Шлюз: 62.33.111.1
        iii) Адрес IPv6/Маска: 2a02:f800:f9:f4::f12/64
        iv) Шлюз: 2a02:f800:f9:f4::f1

v) Делегируемый префикс: 2a02:f800:f5::/48
vi) AS: 20485

d) PURPLE
i) Адрес IPv4/Маска: 2.2.1.101/24
ii) Шлюз: 2.2.1.1
iii) Адрес IPv6/Маска: 2a01:cb00:d:e::101/64
iv) Шлюз: 2a01:cb00:d:e::1
v) Делегируемый префикс: 2a01:cb00:e:1000::/56
vi) AS: 3215

e) MOOGLE
i) Префиксы IPv4: 172.110.32.0/21, 172.217.0.0/16, 8.8.8.0/24
ii) Префиксы IPv6: 2001:4860::/32, 2600:1900::/28
iii) AS: 15169
iv) Адрес IPv4 глобального DNS сервера: 8.8.8.8
v) Адрес IPv6 глобального DNS сервера: 2001:4860:4860::8888

f) ROAMING
i) Адрес IPv4/Маска: DHCP (12.12.12.0/24)
ii) Шлюз: DHCP (12.12.12.1)
iii) Адрес IPv6/Маска: DHCP
iv) Шлюз: DHCP
v) AS: 7018

g) Провайдеронезависимые (PI) адреса и ASN в центральном офисе
i) Адрес IPv4/Маска: 203.0.113.0/24
ii) Адрес IPv6/Маска: 3001:2:3::/48
iii) AS: 64500

6) На провайдерах Gostelecom и Gigafon сделаны настройки BGP.
a) Соседство устанавливается по IPv4 с адреса шлюза на выделяемый провайдером адрес через физический интерфейс и указанные выше номера автономных систем.
b) Все провайдеры анонсируют делегируемые префиксы в “интернет”.
c) Провайдеронезависимый префикс не анонсируется.

7) Настройки VLAN на виртуальных коммутаторах гипервизора уже произведены заранее согласно Топологии L2 и L3. Виртуальные машины подключены в корректные подсети.

ИНСТРУКЦИИ ДЛЯ УЧАСТНИКА

В первую очередь рекомендуется прочитать задание полностью. Следует обратить внимание, что задание составлено не в строгом хронологическом порядке. Для выполнения некоторых пунктов задания может потребоваться выполнение действий из других пунктов, которые изложены в задании ниже. Таким образом, порядок выполнения задания и распределение временных затрат определяется участниками самостоятельно. При разработке плана выполнения задания следует учитывать ежедневную процедуру оценки и перечень технологий, работоспособность которых будет проверяться.

Конкурсное задание имеет сквозную структуру, и предполагается, что вы продолжаете его выполнение во второй и последующие дни с того момента, на котором остановились в предыдущий. Вам доступно полное задание на все конкурсные дни.

Рекомендуется тщательно проверять результаты своей работы. В частности, рекомендуется убедиться в полной работоспособности служб DNS для клиентских устройств.

Также учтите, что в конце каждого дня участникам необходимо в присутствии эксперта выключить все виртуальные машины, сделать их снэпшоты, а затем включить виртуальные машины в желаемом порядке. Сетевое оборудование будет перезагружено по питанию. Также рабочее место может быть выключено в ночное время.

IP адресация в топологии остается на ваше усмотрение, за исключением адресов, предоставляемых провайдерами. Например, для сервера DC1 в сети WINA вы может использовать адреса 172.16.10.156 или 192.168.0.12. Однако, вы должны самостоятельно убедиться, что разработанные схемы адресации соответствуют требованиям задания.

Виртуальные машины могут иметь предустановленное программное обеспечение, которое будет применяться при проверке и оценке, его не рекомендуется удалять.

Доступ ко всем виртуальным Linux-машинам настроен по аккаунту *root:toor*.

При первом доступе к Windows-машинам следуйте инструкциям мастера. В любом случае на всех машинах обеспечьте работоспособность учетной записи *Administrator/P@ssw0rd* с правами как локального, так и доменного администратора.

Если Вам требуется установить пароль, не указанный в задании, а также в инструкциях и файлах дополнений, используйте: P@ssw0rd.

Сетевое оборудование доступно по сети через протокол Telnet из локальных сетей соответствующего офиса.

R1 - 192.168.0.1/24, ASA - 192.168.0.2/24, S1 - 192.168.0.3/24, S2 - 192.168.0.4/24, используется VLAN 13. Получить доступ можно с машины LINCLI1.

R2 - 192.168.0.1/24. Получить доступ можно с машины LINCLI2.

Пароль для подключения и на enable**: wsr**

ЗАДАЧИ И ТЕХНОЛОГИИ, РАБОТОСПОСОБНОСТЬ КОТОРЫХ ОЖИДАЕТСЯ В ДЕНЬ 1

Базовая настройка

1) Настройте имена всех устройств и виртуальных машин в соответствии с топологией.
2) IPv4-адресацию локальных сетей разработайте самостоятельно с учётом следующих требований:
    a) Используйте минимально достаточный размер подсетей:
    b) Количество устройств в сети WINA- до 200.
    c) Количество устройств в сетях WINB, LINA - до 100.
    d) Количество устройств в сети LINB - до 50.
    e) Количество устройств в сети LINRTR- до 25.
    f) Используйте частные диапазоны IP адресов там, где это необходимо.
    g) Устройства в сети DMZ должны использовать провайдеронезависимый (PI) диапазон IP адресов.
3) IP-адреса для связи с провайдерами указаны в разделе “Преднастройка”
    a) На провайдерах дополнительно уже настроен BGP, однако, его использование в этот день не требуется.

Настройка сети центрального офиса

1) Коммутация должна быть настроена согласно Топологии L2.
    a) Транки между коммутаторами S1 и S2 должны формироваться по DTP (где S1 инициирует согласование транка, а S2 ожидает согласования).
    b) Все остальные транки должны быть настроены в режиме on, а DTP отключен в явном виде.
    c) Устройства должны быть в соответствующих сетях VLAN.
    d) Все без исключения неиспользуемые порты коммутаторов должны быть принудительно выключены.
    e) В качестве native VLAN на всех сетевых устройствах используйте VLAN 99.
    f) Настройка Etherchannel в текущий день не требуется.
2) Должна быть обеспечена связь всех устройств внутри локальной сети центрального офиса, а также доступ в интернет для всех пользователей.
    a) Для частных адресов необходимо настроить NAT.
    b) Используемые адреса должны сопоставляться с доменными именами.
    c) IPv6 в организации ещё не внедряется, хотя провайдеры уже его поддерживают.
3) Маршрутизация между VLAN должна быть настроена на R1 и на ASA.
    a) Номера подынтерфейсов должны совпадать с номерами VLAN.
    b) Описание интерфейсов на ASA и подынтерфейсов на R1 должны совпадать с названиями сетей в Топологии L3.
    c) Для выхода в интернет может использоваться любой из двух каналов связи.
    d) Предпочитаемым каналом связи считается Gigafon.

e) Автоматическое переключение на резервный канал в этот день не требуется.

4) Ко всем сетевым устройствам должен быть обеспечен доступ по SSHv2.

a) Доступ должен осуществляться с логином **audit** и паролем **test**

b) При удалённом подключении к системе с этой учётной записью должны быть сразу доступны максимальные полномочия (15-й уровень)

5) Все клиентские устройства (WINCLI3, WINCLI4, LINCLI1) должны получать адреса по DHCP

a) В качестве DHCP-сервера должен выступать DC1.

b) При необходимости в качестве DHCP Relay должен выступать роутер R1.

c) В качестве DNS-сервера должен выступать DC1.

6) В сети центрального офиса должен быть поднят домен **skill39.wsr**

a) DC1 должен быть основным контроллером домена;

b) в домене должны быть созданы подразделения Experts, Competitors, Managers, Visitors, IT;

c) в соответствующих подразделениях должны быть созданы доменные группы: Experts, Competitors, Managers, Visitors, IT.

d) в домене должны быть созданы пользователи согласно файлу **userlist.csv** (файл на рабочем столе DC1):

1) Вся имеющаяся в файле информация о пользователях должна быть внесена в Active Directory;
2) Пользователи должны быть помещены в соответствующие подразделения и группы;
3) все созданные учетные записи должны быть включены и доступны; имя входа пользователя должно строиться по следующему принципу - фамилия+первая буква имени+@skill39.wsr. Например, IvanovI@skill39.wsr.

7) DC2 должен быть членом домена **skill39.wsr.**

8) На DC2 должна быть настроена роль WDS, с помощью которой необходимо установить операционную систему на WINCLI3 и WINCLI4:

a) используйте дистрибутив Microsoft Windows 10 Enterprise, находящийся на одном из жестких дисков DC2;

b) компьютеры должны автоматически стать членами домена с указанными на схеме именами.

9) При первом входе пользователей в домен должна быть отключена приветственная анимация.

10) Все члены домена должны отвечать на запросы по протоколу ICMP.

11) На всех клиентах домена должен быть отключен “Спящий режим”, причем пользователи домена не должны иметь возможность каким-либо образом включить этот режим.

12) На DC1 должен быть настроен DNS-сервер.

a) Сервер должен обслуживать зону **skill39.wsr.**

b) Разрешение имен необходимо организовать в соответствии с Таблицей 1.

c) Запросы, которые выходят за рамки зоны **skill39.wsr** должны пересылаться DNS-серверу MOOGLE. Для проверки используйте адрес **worldskills.ru**.

13) На виртуальной машине LINDMZ должен быть настроен веб-сервер NGINX

a) Используйте стандартный порт протокола HTTP.

b) Файлы веб-сайта должны располагаться в каталоге **/var/www/.**

c) В качестве страницы по умолчанию создайте файл index.html со следующим содержимым:

```
<html><body>
    <h1>Welcome to DigitalSkills!</h1>
    <h3>Server LINDMZ</h3>
</body></html>
```

d) Сайт должен быть доступен по доменному имени **web.skill39.wsr** для клиентов локальной сети центрального офиса.

e) Сайт должен быть доступен только по доменному имени, при запросе по IP адресу должна отображаться страница ошибки с кодом 404.

Настройка сети филиала 1

1) Должна быть обеспечена связь всех устройств внутри локальной сети филиала, а также доступ в интернет для всех пользователей филиала.

2) На виртуальной машине SRV2 должен быть настроен DNS-сервер с учетом следующих требований:

a) Сервер должен обслуживать зону **ext.skill39.wsr.**

b) Разрешение имен необходимо организовать в соответствии с Таблицей 1.

c) Запросы, которые выходят за рамки зоны **skill39.wsr** должны пересылаться DNS серверу MOOGLE. Для проверки используйте адрес **worldskills.ru.**

d) Файлы зон должны располагаться в каталоге **/var/dns/.**

3) На маршрутизаторе R2 должен быть настроен сервер DHCP для локальной сети:

a) Используете адрес SRV2 в качестве адреса DNS-сервера для клиентов сети.

b) Используйте DNS-суффикс **ext.skill39.wsr.**

4) Должно работать соединение Serial между филиалом 1 и центральным офисом.

a) Для связи необходимо использовать протокол PPP

b) Также необходимо использовать взаимную аутентификацию по CHAP

c) Весь трафик из филиала 1 до сервера DC1 (по адресу **dc1.ext.skill39.wsr**) должен передаваться через это соединение.

Настройка сети филиала 2

1) На виртуальной машине LINRTR должен быть настроен сервер протокола динамической конфигурации хостов для локальной сети:

a) Используете адрес LINRTR в качестве адреса DNS сервера для клиентов сети.

b) Используйте DNS суффикс **skill39.wsr.**

2) LINRTR должен выполнять трансляцию DNS запросов (DNS Proxy) от локальных клиентов на

сервер MOOGLE.
3) LINRTR должен обеспечивать доступ в Интернет для клиентов сети.
4) WINCLI1 должен быть членом рабочей группы PURPLE.
5) На WINCLI1 должны существовать две активные учетные записи: Administrator/P@ssw0rd, User/P@ssw0rd1. Первая учетная запись должна быть членом группы локальных администраторов компьютера, вторая - членом группы пользователей компьютера.
6) На WINCLI1 должен быть отключен “Спящий режим”, причем члены группы пользователей компьютера не должны иметь возможность каким-либо образом включить этот режим.

Настройка мобильных клиентов

1) На WINNET должен быть отключен “Спящий режим”, причем члены группы пользователей компьютера не должны иметь возможность каким-либо образом включить этот режим.

По завершению рабочего дня

1) В конце рабочего дня необходимо будет снять снэпшоты всех виртуальных машин в топологии с названием AfterDay1, а на сетевых устройствах сделать резервную копию в файл **after-day1.cfg.**
2) После завершения выполнения задания будет проведена автоматизированная проверка результатов.
3) Все проверки будут выполняться исключительно по доменным именам. Подключение к сетевым устройствам будет производиться по протоколу SSH.
4) В случае, если устройство или виртуальная машина недоступны по какой-либо причине (не подходят учётные записи, оговоренные в задании, нет сетевой связности), дальнейшая проверка этого устройства не проводится.

ЗАДАЧИ И ТЕХНОЛОГИИ, РАБОТОСПОСОБНОСТЬ КОТОРЫХ ОЖИДАЕТСЯ В ДЕНЬ 2

Базовая настройка

1) Спланируйте и настройте IPv6 адреса на всех устройствах и виртуальных машинах.
   a) Используйте диапазоны IP адресов, делегируемые провайдерами. Они указаны в разделе “Преднастройка”
   b) В центральном офисе все устройства и машины должны использовать провайдеронезависимый (PI) диапазон IP адресов.
2) Необходимо обеспечить доступ ко всем веб-сайтам по IPv6.
3) На всех сетевых устройствах время должно быть синхронизировано с сервером MOOGLE и должно отображаться в московском часовом поясе.
4) На всех серверах и клиентах в центральном офисе время должно быть синхронизировано с сервером MOOGLE и должно отображаться в московском часовом поясе.

Настройка сети центрального офиса

1) Для выдачи адресов в сети WINA и WINB настройте DHCPv6-сервер на DC1 и обеспечьте его отказоустойчивость с помощью DC2. Вместе с тем отказоустойчивость должна быть обеспечена и для всех областей DHCPv4.
2) DC2 должен быть резервным контроллером домена **skill39.wsr**. Роль **RID pool manager** должна быть передана на этот сервер. Реплику глобального каталога должен нести только DC1.
3) На DC2 должны быть переданы все DNS-зоны с DC1.
4) На DC1 и DC2 с SRV2 должна быть передана DNS-зона **ext.skill39.wsr**
5) В сети LINA должен работать SLAAC.
6) В качестве DNS-серверов все клиенты сетей WINA, WINB и LINA должны использовать DC1 и DC2.
7) На всех виртуальных машинах и сетевых устройствах в сети центрального офиса должен быть включен мониторинг.
   a) Опрос всех устройств будет производиться с машины SRV1.
   b) Достаточно использовать SNMPv2c.
   c) Используйте строку сообщества **notpublic** в режиме “только чтение”
8) Должна быть обеспечена связь между внутренними сетями центрального офиса и филиалами 1 и 2 через интернет с помощью GRE-туннелей.
   a) В центральном офисе на маршрутизаторе R1 должны быть созданы два туннельных интерфейса с номерами 0 и 1.
   b) Туннель с номером 0 должен использоваться для связи с R2.
   c) Туннель с номером 1 должен использоваться для соединения по GRE с виртуальной машиной LINRTR
   d) GRE-туннель на LINRTR должен устанавливаться при загрузке операционной системы.
   e) Прямое последовательное соединение между центральным офисом и филиалом будет демонтировано в конце дня.
   f) Для обеспечения маршрутизации IPv4 между центральным офисом и филиалами поверх туннелей необходимо использовать протокол OSPFv2
   g) Дополнительно настройте OSPFv3 между R1 и R2 для обмена маршрутами IPv6.
   h) Весь трафик между центральным офисом и филиалами должен передаваться через GRE-туннели.
9) Протоколы динамической маршрутизации на компьютерах под управлением ОС Linux должны использовать пакет quagga.

10) Выход в интернет должен обеспечиваться бесперебойно.

a) В случае сбоя у провайдера должно происходить автоматическое переключение на резервный канал.

b) В случае сбоя одного из провайдеров у пользователей должен работать интернет хотя бы по протоколу IPv4.

c) В случае сбоя одного из провайдеров серверы LINDMZ и WINDMZ должны быть доступны из интернета хотя бы по протоколу IPv4.

11) Интерфейсы F0/4 и F0/5, соединяющие коммутаторы, необходимо объединить в Etherchannel.

a) Канал должен согласовываться с помощью LACP. S2 должен ждать согласования, а S1 его инициировать.

b) Трафик сетей WINA, WINB, LINA должен ходить через этот канал. Трафик сети DMZ должен ходить через интерфейс F0/3, не входящий в Etherchannel

12) Необходимо обеспечить отказоустойчивость локальной сети:

a) Корнем STP во всех настроенных VLAN должен быть коммутатор S1.

b) В случае сбоя или изменения в коммутации пересчёт STP должен происходить в течение 10 секунд.

c) В случае сбоя соединения между коммутаторами трафик всех сетей должен ходить по оставшимся каналам.

d) Сервер LINDMZ должен получать маршрут по умолчанию динамически по протоколу BGP от R1 и ASA.

e) R1 и ASA должны анонсировать в сторону LINDMZ только маршрут по умолчанию и фильтровать другие префиксы.

f) Входящий трафик из интернета до сервера LINDMZ должен приходить через R1 и переключаться на ASA только в случае сбоя у провайдера.

13) Виртуальная машина SRV1 должна предоставлять сервис удаленного доступа на основе технологии OpenVPN с учетом следующих требований:

a) Устройство TUN.

b) Протокол UDP.

c) Порт сервера 8081.

d) Применяется дополнительная TLS аутентификация.

14) На виртуальной машине LINDMZ должна быть добавлена поддержка протокола IPv6 для веб-сервера NGINX.

a) Веб-сайт **web.skill39.wsr** должен быть также доступен по доменному имени **web.skill39.ru** по протоколу IPv4 для клиентов в интернете.

b) Веб-сайт **web6.skill39.wsr** должен быть доступен по доменному имени только по протоколу IPv6 для всех клиентов в сети центрального офиса и по доменному имени **web6.skill39.ru** по протоколу IPv6 для клиентов в интернете.

c) Для обеспечения работы доменных имён **web.skill39.ru** и **web6.skill39.ru** необходимо зарегистрировать их на сайте **nic.moogle.ru**, указав актуальные IP-адреса сервера.

d) Файлы веб-сайта **web6** должны располагаться в каталоге **/var/www/ip6**.

e) В качестве страницы по умолчанию для сайта **web6** создайте файл **index.html** со следующим содержимым:

```
<html><body>
    <h1><font color=green>Your network is READY for IPv6!</font></h1>
    <h3>Server LINDMZ</h3>
</body></html>
```

15) На виртуальной машине WINDMZ используйте только протокол IPv6.
16) На виртуальной машине WINDMZ настройте роль web-сервера и разместите на нем сайт со следующей конфигурацией:

a) в качестве страницы по умолчанию создайте файл **index.html** со следующим содержимым:

```
<html>
    <body>
        <b>It`s a first project!</b>
    </body>
</html>
```

b) сайт должен быть доступен по доменному имени **project.skill39.wsr** для всех клиентов в сети центрального офиса.

c) сайт должен быть доступен по доменному имени **project.skill39.ru** для клиентов в интернете.

d) для обеспечения работы доменного имени **project.skill39.ru** необходимо зарегистрировать доменное имя на сайте **nic.moogle.ru**, указав актуальный IPv6-адрес сервера.

17) В домене **skill39.wsr**:

a) на сервере DC2 с использованием двух свободных жестких дисков создайте RAID0-массив. Для доступа к нему используйте букву **G:**

b) создайте общую папку **g:\shares\users**:

c) Все пользователи домена, кроме членов группы Visitors, должны иметь права на запись в эту папку;

d) Члены группы Visitors не должны иметь прав доступа к этой папке;

e) Запретите выполнение любого программного кода из указанной папки (учтите, что пользователи не должны лишиться возможности сохранять исполняемые файлы);
ограничьте объем указанной папки до **100 Мб**.

Настройка сети филиала 1

1) На виртуальной машине SRV2 должна быть включена поддержка протокола IPv6 для службы DNS с учетом следующих требований:

a) Сервер должен обслуживать зону **ext.skill39.wsr**.

b) Разрешение имен необходимо организовать в соответствии с Таблицей 1.

c) Запросы, которые выходят за рамки зоны **skill39.wsr** должны пересылаться DNS серверу MOOGLE. Для проверки используйте адрес **ip6.worldskills.ru**.

d) Настройте подчиненную зону (Secondary DNS) для зоны **skill39.wsr**.

e) Реализуйте поддержку разрешения обратной зоны в соответствии с Таблицей 1.

2) На виртуальной машине SRV2 должен быть настроен веб-сервер Apache2.

a) Используйте стандартный порт протокола HTTP.

b) Файлы веб-сайта должны располагаться в каталоге **/var/www/**.

c) В качестве страницы по умолчанию создайте файл index.html со следующим содержимым:

```
<html><body>
    <h1>Welcome to DigitalSkills!</h1>
```

<h3>Server SRV2</h3>
</body></html>

d) Сайт **ext.skill39.wsr** должен быть доступен по доменному имени по протоколу IPv4 для всех клиентов в сети центрального офиса.

Настройка сети филиала 2

1) Виртуальная машина LINRTR должна обеспечивать автоматическое предоставление настроек IPv6 для клиентов локальной сети.

a) Клиенты сети должны иметь доступ к сайтам, работающим по протоколам IPv4 и IPv6. Для проверки можете использовать адрес **moogle.ru** и **ip6.moogle.ru**.

2) Должна выполняться односторонняя синхронизация файлов веб-сайтов с LINDMZ на сервер SRV2.

a) Период синхронизации - 1 минута.

b) Каталог для синхронизации на LINDMZ - **/var/www**

c) Каталог для синхронизации на SRV2 - **/var/www**

d) Файлы на SRV2 должны обновляться, но не удаляться при их отсутствии на LINDMZ.

e) Файлы **index.html** должны быть исключены из синхронизации. Изначальная информация в этих файлах на SRV2 должна быть сохранена.

Настройка мобильных клиентов

1) На виртуальной машине WINNET:

a) Установите клиент удаленного доступа на основе технологии OpenVPN.

b) Сформируйте конфигурационный файл **client.ovpn** в каталоге **C:\vpn** для автоматизации установления VPN соединения.

c) При подключении к VPN серверу не должен запрашиваться ввод дополнительных параметров.

d) После установления VPN соединения WINNET должен иметь возможность доступа к локальным ресурсам сети по доменным именам зоны **skill39.wsr.**

По завершению рабочего дня

1) В конце рабочего дня необходимо будет снять снэпшоты всех виртуальных машин в топологии с названием AfterDay2, а на сетевых устройствах сделать резервную копию в файл **after-day2.cfg.**
2) После завершения выполнения задания будет проведена автоматизированная проверка результатов.
3) Все проверки будут выполняться исключительно по доменным именам. Подключение к сетевым устройствам будет производиться по протоколу SSH.
4) В случае, если устройство или виртуальная машина недоступны по какой-либо причине (не подходят учётные записи, оговоренные в задании, нет сетевой связности), дальнейшая проверка этого устройства не проводится.

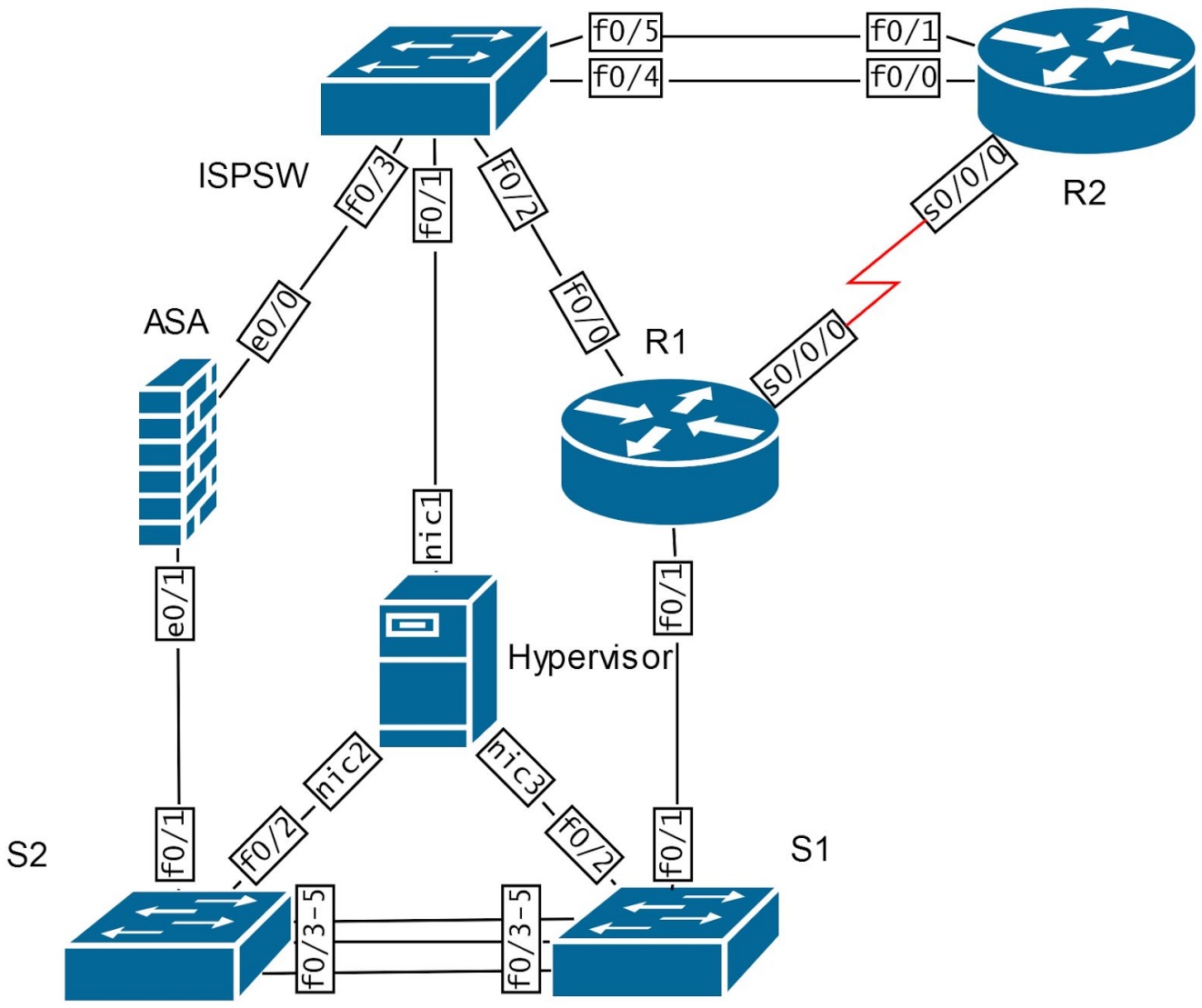
Таблица 1 - Настройки служб DNS

Устройство	Доменное имя	Тип записи
DC1	dc1.ext.skill39.wsr	A
DC1	dc1.skill39.wsr	A, AAAA, PTR
DC2	dc2.skill39.wsr	A, AAAA, PTR
WINCLI3	wincli3.skill39.wsr	A, AAAA, PTR
WINCLI4	wincli4.skill39.wsr	A, AAAA, PTR
WINDMZ	project.skill39.wsr	AAAA, PTR
WINDMZ	project.skill39.ru	AAAA
LINDMZ	web.skill39.wsr	A
LINDMZ	web6.skill39.wsr	AAAA
LINDMZ	web.skill39.ru	A
LINDMZ	web6.skill39.ru	AAAA
SRV1	srv1.skill39.wsr	A
SRV2	ext.skill39.wsr	A, AAAA, PTR
LINRTR локальный IP	linrtr.skill39.wsr	A
LINRTR глобальный IP	br2.skill39.wsr	A
R1	r1.skill39.wsr	A
ASA	asa.skill39.wsr	A
S1	s1.skill39.wsr	A
S2	s2.skill39.wsr	A
R2	r2.ext.skill39.wsr	A

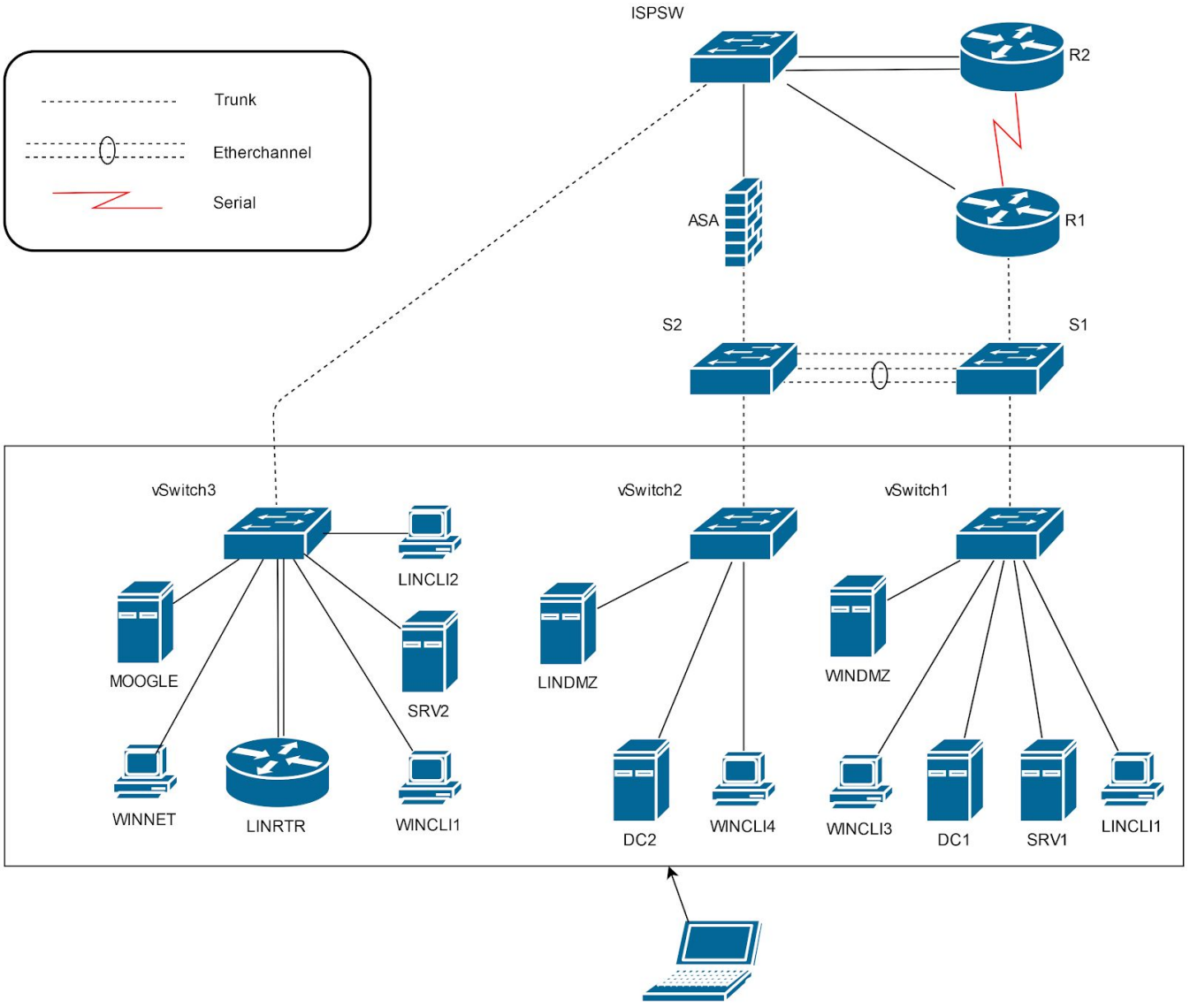
Таблица 2. Правила журналирования

Устройство	Тип сообщений	Файл
LINDMZ, SRV1	auth, authpriv	/opt/logs/auth/<hostname>
R1, S1, S2, ASA	Все notification и более важные	/opt/logs/net/<ip>
SRV1, SRV2, LINDMZ	Error и более важные	/opt/logs/linsrv/<hostname>

Топология L1



Топология L2



Топология L3