


V РЕГИОНАЛЬНЫЙ ЧЕМПИОНАТ «АБИЛИМПИКС»

СОГЛАСОВАНО
Региональным центром развития
движения «Абилимпикс»
в Пермском крае

 - Г.А. Ключева

КОНКУРСНОЕ ЗАДАНИЕ

по компетенции «Сетевое и системное администрирование»

г. Пермь, 2020 г.

ВВЕДЕНИЕ

КОНКУРСНОЕ ЗАДАНИЕ

Позвольте представиться, мой новый коллега: Я начальник ИТ-департамента успешной финансовой корпорации «ЦИС и Ко Финанс», куда вы только что устроились на должность главного системного администратора. Благодаря соблюдению правил регуляторов и собственным строгим внутренним правилам, в кризисное время наша компания сохраняет стабильность, о чем свидетельствует ваша немалая зарплата. К сожалению, ваш коллега, создававший ИТ-инфраструктуру, находится в длительной командировке и еще не успел ввести Вас в курс всех дел. Однако благодаря вашей высокой квалификации вам должно хватить и тех обрывков информации, что он успел передать.

В Ваш первый рабочий день необходимо провести подключение нового офиса, открытие которого назначено на начало следующей недели, к нашей корпоративной сети. После этого наладить связь с остальными офисами компании. В Вашем распоряжении в данный момент имеется:

- 2 коммутатора Cisco 2 уровня;
- 2 маршрутизатора Cisco;
- один сервер виртуализации.

Остальное оборудование обещано поставить в ближайшие дни.

Сейчас каждый час на счету, а потому наше руководство требует, чтобы все задачи были выполнены сегодня в течении 4 часов.

ЧАСТЬ 1. ПОДКЛЮЧЕНИЕ И НАСТРОЙКА СЕТЕВОГО ОБОРУДОВАНИЯ

Прежде, чем приступить к работе важно:

- ознакомиться со схемой подключения Схема 1;
- **ВНИМАТЕЛЬНО** и **ЦЕЛИКОМ** прочитать задание;
- не обязательно выполнять пункты задания по очереди, а также задание целиком, Вам может не хватить на это времени. Исходя из этого подумайте, как оптимизировать свою работу.

!!! ВНИМАНИЕ !!!

По окончании работы Вам необходимо предоставить на проверку сетевое оборудование в **выключенном** состоянии.

В любом случае все предоставленное Вами оборудование будет перезагружено экспертами перед началом проверки.

В случае невозможности входа в систему, выполнение работы экспертами по данной части конкурсного задания не оценивается.

При выполнении задания учтите возможные внештатные кратковременные или длительные отключения электроэнергии.

1. Произведите подключения сетевого оборудования согласно Схеме 1;
2. Для настройки устройств используйте следующие параметры сетей (где N – номер участника):
 - a. Сеть Центрального офиса LAN1: 172.16.N.16/25;
 - b. Сеть Офиса Северный LAN2: 172.16.N.128/26;
 - c. Сеть Офиса Таёжный LAN3: 172.16.N.192/27;
 - d. Сеть ISP: 10.0.N.64/30;
 - e. Сеть управления MNG: 176.18.N.48/28;
3. Настройте сетевые адаптеры ПК SERVER согласно Схеме 1;
4. Известно, что маршрутизатор R1 переехал из старого офиса компании и его IP-адрес 10.0.250.254/24, а пароль консольного подключения

cisco. Согласно правилам определения имен устройств в компании назовите маршрутизатор Central-Router.

5. Установите пароли с функцией требования их ввода (при необходимости):

- на привилегированный режим **ciscoen**
- на первые 5 терминальные линии: **networkvty**
- на консольное подключение: **letmein**

Не забудьте включить шифрование паролей на устройствах с помощью специального сервиса;

6. Роутер R2 был куплен специально для подключения нового офиса. Его конфигурация не тронута и находится в состоянии по умолчанию. Назовите маршрутизатор Taiga-Router. Установите такие же пароли доступа, как и на роутере Central-Router;

7. Известно, что коммутаторы SW1 и SW2 также переехали из старого офиса компании, но их конфигурации сброшены. Назовите их Central-MainSW и Central-SW2 соответственно. Установите такие же пароли доступа, как и на роутере;

8. Для централизованного конфигурирования VLAN в коммутируемой сети предприятия используйте протокол VTP версии 3; в качестве основного сервера VTP настройте Central-MainSW; в качестве домена используйте **VTPFinCorp.ru**; используйте пароль **VTPPass** для защиты VTP. Таблица VLAN должна содержать следующие сети:

- сеть локальной сети LAN1 – VLAN 10, с именем LAN1;
- сеть управления MNG – VLAN 20, с именем MANAGEMENT;
- сеть неиспользуемых портов – VLAN 30, с именем DEPO;

9. Настройте IP-адреса коммутаторов соответственно Схеме 1. Используйте ВЛВС 20 в качестве сети управления сетевым оборудованием. Все неиспользуемые интерфейсы отключите и переведите в VLAN 30;

10. Включите протокол безопасности port security на интерфейсе fa0/8; максимальное количество MAC адресов на порту должно быть равно 10; MAC адреса должны оставаться в настройках после перезагрузки; способ обработки нарушения безопасности – блокировка без уведомления;

11. На всех сетевых устройствах используется модель AAA. На виртуальных линиях с паролем используется протокол SSHv2, доступ по telnet отключен для предотвращения утечки информации. Пользователь для авторизации **admin / Adminin!**

Он должен обладать максимальными привилегиями. Все коммутаторы и маршрутизаторы должны быть в домене **FinCorp.ru**;

12. Между коммутаторами необходимо обеспечить отказоустойчивость с помощью протокола RAgP: организовать агрегацию между портами согласно Схеме 1 с номером агрегированного интерфейса 2;

13. Настройте интерфейсы маршрутизаторов согласно Схеме 1. На интерфейсе роутера центрального офиса реализуется технология RoS (роутер-на-палочке). Используйте подынтерфейсы 10 и 20 для сетей Lan1 и MNG соответственно;

14. Используя списки контроля доступа (ACL) обеспечьте, чтобы удаленное подключение к маршрутизатору было возможно только с компьютера участника, но при этом никак не ограничивало трафик через маршрутизатор;

15. Настройте динамическую маршрутизацию с использованием протокола OSPFv2 согласно Схеме 1, объявите сети с использованием md5 ключа **cisco321** для передачи OSPF-пакетов. Маршрутизаторы должны получать информацию о всех сетях;

16. На обоих маршрутизаторах отключите протокол CDP только на портах в сторону сети ISP;

17. На всех сетевых устройствах должны быть настроены: вывод консольных сообщений в синхронном режиме, чтобы выводимые сообщения не разрывали ввод команд в консоли; баннер «Сообщение дня» (message-of-the-day) следующего содержания: «Authorized access only!»;

18. В сетевой инфраструктуре сервером синхронизации времени является Central-Router. Все остальные сетевые устройства должны использовать его в качестве сервера времени. Настройте временную зону с названием MSK, укажите разницу с UTC +5 часов. Используйте стратум 2. Используйте для синхронизации клиентов аутентификацию MD5 с ключом **timestamp** ;

19. На Central-Router настройте протокол динамической конфигурации хостов для сети LAN2. Устройства должны получать корректные ip/netmask и gateway. Компьютер CENTOS должен получать адрес 172.16.N.138;

20. С ПК Server должен обеспечиваться доступ ко всем сетевым устройствам.

ЧАСТЬ 2. УСТАНОВКА И НАСТРОЙКА ОС

Прежде, чем приступить к работе важно:

- ознакомиться со схемой подключения Схема 1;
- **ВНИМАТЕЛЬНО** и **ЦЕЛИКОМ** прочитать задание;
- не обязательно выполнять пункты задания по очереди, а также задание целиком, Вам может не хватить на это времени. Исходя из этого подумайте, как оптимизировать свою работу.

!!! ВНИМАНИЕ !!!

Все необходимые дистрибутивы расположены на рабочем столе ПК

По окончании работы Вам необходимо предоставить на проверку виртуальные машины в выключенном состоянии.

В любом случае все VM будут перезагружены экспертами перед началом проверки.

В случае невозможности входа в систему выполнение работы экспертами по данной части конкурсного задания не оценивается.

При выполнении задания учтите возможные внештатные кратковременные или длительные отключения электроэнергии.

Установка и настройка ОС семейства Windows

1. Создайте VM со след. параметрами: имя VM - DC; объем ОП 4 гб; 4 ядра процессора; виртуальный Intel VT-x/EPT или AMD-V/RVI; тип подключения сетевого адаптера – VMnet0 (автомост); подключите диск с установленной ОС Win Server 2016 (пароль учетной записи Администратор: **Adminin!**)
2. Настройте сетевые параметры согласно Схеме 1;
3. Настройте роль контроллера домена для домена **FinCorp.ru**.
Создайте организационные единицы, группы и пользователей в домене FinCorp.ru согласно таблице:

| Уч. запись | Пароль | Подразделение | ФИО | Член групп |
|-------------------|---|----------------------|--------------------|---|
| admin | Abx0000! (срок действия пароля не ограничен) | Central/Admins | Бова Королевич | Администраторы; Администраторы домена; Администраторы предприятия |
| User1 | Abx1111! (запретить смену пароля пользователем; срок действия пароля не ограничен) | Central/Sales | Илья Муровец | Пользователи домена; Central_Sales |
| User2 | Abx2222! (запретить смену пароля пользователем; срок действия пароля не ограничен) | Central/Managers | Добрыня Никитич | Пользователи домена; Central_Managers |
| User3 | Abx3333! (запретить смену пароля пользователем; срок действия пароля не ограничен) | North/ North_IT | Алеша Попович | Пользователи домена; North_IT |

4. Установите и настройте службы DNS и DHCP для сети LAN1. Служба DHCP должна иметь пул из 10 адресов, начиная с 5-го доступного адреса из сети LAN1, исключая 6 и 7 адрес; 4-ий адрес диапазона DHCP должен быть зарезервирован для машины Central-RDS. В параметрах передается шлюз и DNS сервер; службу DNS настройте на серверы пересылки: 8.8.8.8 и 8.8.4.4;

5. Настройка VM RDS: Назовите сервер «Central-RDS»; ОС должна получать зарезервированный IP-адрес от Central-DC согласно Схеме 1;

6. Введите ПК Central-RDS в домен FinCorp.ru. В структуре AD переместите его в подразделение Central;

7. На ПК Central-RDS настройте:

- терминальный сервер с лицензированием по компьютерам (используйте временную лицензию);
- веб доступ RemoteApp к службам терминалов сервера;
- публикацию программы «WordPad» на веб-портале RemoteApp для всех сотрудников отдела North_IT.

8. Обеспечьте отказоустойчивое хранилище на сервере CO-DC, создав зеркальный рейд, добавив два диска по 1 GB (RAID 1). Назначьте ему букву **D:** ;

9. На сервере Central-DC создайте сетевые папки, настройте фильтры блокировки файлов (запретить хранение исполняемых файлов, системных файлов, файлов аудио и видео) в соответствии с таблицей:

| Папка | Группы файлов для блокировки | Квотирование |
|------------------|--|--|
| D:\Folders\Sales | Исполняемые файлы; Системные файлы; Файлы аудио и видео; | Жесткая квота Порог: 50МБ с расширением 50Мб |
| D:\Folders\IT | Нет | Нет |

10. Настройте и примените групповые политики к пользователям и клиентским рабочим станциям домена:

10.1. Создайте политику учетных записей для всех пользователей домена FinCorp.ru:

- вести журнал паролей - 9;
- максимальный срок действия пароля - 40;

- пароль должен отвечать требованиям сложности - выключено;
- минимальная длина пароля – 8;
- продолжительность блокировки учетной записи - 7;
- пороговое значение блокировки - 5;
- время до сброса счетчика блокировки - 1;

10.2. добавьте пользователей отдела North / North_IT в локальную группу администраторов для всех компьютеров (ноутбуков) домена FinCorp.ru;

10.3. Подключите сетевые папки с файлового сервера как диски Net_Share_Sales - сетевую папку \\Central-DC.FinCorp.ru\ Sales как диск **D:** для сотрудников всех отделов Sales, входящих в домен FinCorp.ru;

10.4. включите удаленный рабочий стол на всех компьютерах, находящихся в данный момент в филиале North (RDP_ON).

Установка и настройка ОС семейства Linux

11. На VM Debian установить следующие параметры:

имя пользователя: user;

пароль для пользователя user: **Abx1111!**

12. Задайте имя компьютера: North-Debian;

13. Измените DNS-суффикс для данной машины на russia.ru;

14. Настройте сетевой интерфейс согласно Схеме 1.

15. Добавьте для текущего сетевого интерфейса alias с IP согласно Схеме 1;

16. Заведите пользователей user2, user3 пароли соответственно: **Abx2222!, Abx3333!**

17. Создайте группу ablmpx и добавьте в нее пользователя user2;

18. Установите web-сервер Apache. Замените стартовую страницу (стартовая страница должна содержать ТОЛЬКО сообщение «Abx2020»). Доступ к сайту должен осуществляться по имени Abx2020.FinCorp.ru;

19. Загрузите в виртуальную среду готовый образ ОС CentOS 7. Для входа в систему используйте логин/пароль **root/toor**;

20. Задайте имя компьютера: North-CENTOS;

21. Установите пароль на суперпользователя root: **Adminin!**

22. Настройте сетевой интерфейс согласно Схеме 1;

23. Измените DNS-суффикс для данной машины на russia.ru;

24. Разрешите удаленное подключение по протоколу SSH для суперпользователя root.

CXEMA 1

R1:

G0/0 - Последний адрес сети ISP

G0/1 - Последние адреса сетей LAN1 и MNG

G0/2 - Последний адрес сети LAN2

R2:

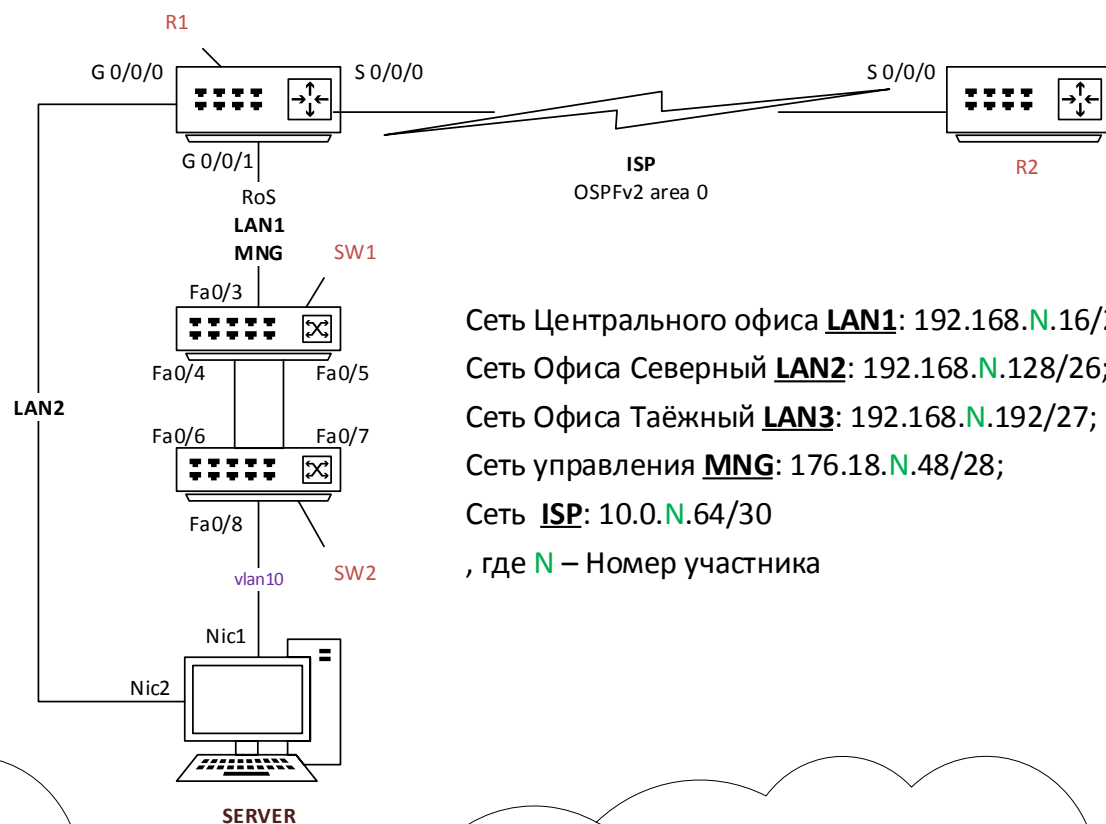
G0/0 - Первый адрес сети ISP

Loopback 22 - Любой адрес сети LAN3

SW1 - Первый адрес сети MNG**SW2** - Второй адрес сети MNG**SERVER:**

Nic1 - Предпоследний адрес сети Lan1;

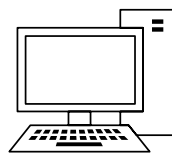
Nic2 - Предпоследний адрес сети Lan2;

DC-C - Четвертый адрес сети Lan1;**RDC** – DHCP client;**Debian-N** – 11ый и 12ый адреса сети Lan2;**CENTOS-N** – DHCP client.Сеть Центрального офиса **LAN1**: 192.168.N.16/25;Сеть Офиса Северный **LAN2**: 192.168.N.128/26;Сеть Офиса Таёжный **LAN3**: 192.168.N.192/27;Сеть управления **MNG**: 176.18.N.48/28;Сеть **ISP**: 10.0.N.64/30, где **N** – Номер участника**ORACLE VIRTUALBOX**

Офис Северный



Debian



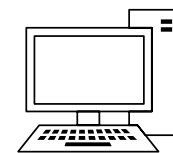
CENTOS

VMWARE WORKSTATION

Центральный офис



DC



RDS

Условия проведения V Регионального чемпионата профессионального мастерства для инвалидов и лиц с ОВЗ «Абилимпикс» по компетенции «Сетевое и системное администрирование» в очном-дистанционном формате

1. Инфраструктура площадки:

Соревнования по компетенции «Поварское дело» проводятся в соответствии со стандартами Абилимпикс. Соревнования проходят на площадке, которая полностью оснащена оборудованием, инструментами и расходными материалами согласно ИЛ по компетенции. На площадке оборудовано 5 рабочих мест для 15 участников из разных ПОО.

Для обеспечения санитарно-эпидемиологической безопасности и равных условий для выполнения задания, все участники будут разведены на два потока: 1 смена и 2 смена в два дня (21 и 22 октября), в каждой смене по 5 человек. Перед каждой сменой в Лаборатории планируются следующие мероприятия:

1. Фильтр участников (замер температуры посредством безконтактного термометра, обработка рук дезинфицирующим средством, обязательный масочный режим)
2. Проветривание помещений площадки
3. Санитарная обработка всех поверхностей, ручек, оборудования на площадке
4. Обработка всех помещений площадки рециркулятором
5. Временной период между сменами не менее 2 часов.

Рабочие места на площадке расставлены таким образом, что между участниками соревнования соблюдается дистанция 1,5 м.

За работой участников наблюдает команда экспертов из 6 человек во главе с главным экспертом. Постоянно на площадке находятся 3 эксперта. Еще 2 эксперта по объективной и субъективной оценке находятся в отдельном помещении. Главный эксперт также находится в отдельном помещении.

2. Проведение соревнований: Проведение соревнований проходит в очном режиме, опираясь на Техническое описание компетенции и Конкурсное задание.

В день С-1 для всех участников и экспертов площадки главный эксперт проводит инструктаж, проводится ознакомление с рабочими местами, распределение по сменам.

В этот же день для 1 смены первого дня (5 человек) проводятся соревнования.

Накануне соревнований участники каждой смены подписывают протоколы по технике

безопасности, главный эксперт формирует у себя пакет документов.

Технический эксперт площадки выдает сырьевой набор участникам.

Участникам каждой смены отводится время на организацию рабочего места (15 минут на подготовку и разбор сырья, а затем 15 минут на подготовку рабочего

места и возможность взять необходимые дополнительные инвентарь и оборудование

из тулбокса).

За таймингом участников следит технический эксперт площадки.

Во время подачи конкурсных блюд, технический эксперт площадки фиксирует

время подачи.

В день С 1 соревнования проводятся для 2 смен: 1 смена второго дня и 2 смена второго дня.

В конце дня С 2 происходит подведение итогов, занесение результатов в протоколы, сдача протоколов.

После соревнований проводится генеральная уборка всех помещений с дезинфицирующими средствами.