



СОГЛАСОВАНО

ФИО
« ____ » _____ 20__ года

подпись

КОНКУРСНОЕ ЗАДАНИЕ

**Региональный Чемпионат
ЮниорПрофи 2020**

Ленинградская область

Сетевое и системное администрирование

Возрастная группа 14+

Конкурсное задание включает в себя следующие разделы:

1. Формы участия в конкурсе
2. Задание для конкурса
3. Задание
4. Критерии оценки

Количество часов на выполнение задания: 12ч.

1. ФОРМЫ УЧАСТИЯ В КОНКУРСЕ

Командный конкурс, команда 2 человека.

2. ЗАДАНИЕ ДЛЯ КОНКУРСА

Содержанием конкурсного задания является Создание и настройка сетевой инфраструктуры предприятия. Участники соревнований получают инструкцию, монтажные и принципиальные электрические схемы. Конкурсное задание сквозное и выполняется в течении 3^x дней.

Конкурс включает в себя монтаж и подключение сетевого и серверного оборудования и выполнение пуско-наладочных работ сетевого и серверного оборудования.

Окончательные аспекты критериев оценки уточняются членами жюри. Оценка производится ежедневно по окончании работ. 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.

ЗАДАНИЕ

День 1. Сетевое задание

После запроса изменить инфраструктуру сети вашего офиса, группа инженеров вашей компании разработала новую схему сети. Настройте оборудование исходя из схемы сети и инструкций.

Будьте внимательны, член команды, который настраивает устройства cisco, может использовать компьютер VPC-L1, но данное устройство имеет также свою роль в сети.

1. Подключите все устройства между собой опираясь на физическую схему сети.

2. Настройте подключение сети на внешнем интерфейсе маршрутизатора **SM-PA-R1** согласно представленной топологии.

3. Для менеджмента вашей сети настройте на всех устройствах имена в соответствии со схемой сети. Обеспечьте доступ к устройствам и Установите пароль на привилегированный режим **junior2020**.

4. Создайте пользователя **SMadmin** на всех устройствах для аутентификации по SSH (SSHv2) для домена **cisco.com**. Для авторизации пользователя через SSH на устройствах установите пароль **sm@ssh**. Пользователь должен обладать максимальными привилегиями. Для увеличения безопасности аутентификация по telnet должна быть невозможна.

5. На всех маршрутизаторах и коммутаторах задайте сообщение при аутентификации о невозможности неавторизованного доступа.

6. Будущая сеть подразумевает синхронизацию часов с сервером синхронизации времени настроенным на маршрутизаторе **SM-PA-R1**. Настройте синхронизацию на всех сетевых устройствах и сервер синхронизации времени на соответствующем маршрутизаторе.

7. Сервера и клиентские машины должны быть логически разделены. Для этого создайте 3 VLAN в центральном офисе с номерами и именами указанными далее. Вы должны использовать инструкции группы инженеров.

a. VLAN 1000, Management, Адрес подсети: 10.1.1.128/25.

Порты назначенные **SM-PA-SW1**: Fa0/20-24

a. VLAN 10, Wserver, Адрес подсети: 10.1.10.0/24

Порты назначенные **SM-PA-SW1**: Fa0/2-9

a. VLAN 20, Workers, Адрес подсети: 10.1.20.0/24

Порты назначенные **SM-PA-SW1**: Fa0/10-19

8. В удаленном офисе вам также потребуется создать 3 VLAN, но адреса подсети меняются таким образом, что второй октет адреса изменяется на 2:

a. VLAN 1000, Management, Адрес подсети: 10.2.1.128/25.

Порты назначенные на **SM-LI-SW1**: Fa0/20-24

a. VLAN 10, Wserver, Адрес подсети: 10.2.10.0/24

Порты назначенные на **SM-LI-SW1**: Fa0/2-9

a. VLAN 20, Workers, Адрес подсети: 10.2.20.0/24

Порты назначенные на **SM-LI-SW1**: Fa0/10-19

9. В обоих офисах шлюз по умолчанию в созданных VLAN должен быть последний адрес сети.

10. Для удаленного подключения коммутаторы должны иметь первый адрес в Management VLAN.

11. Два офиса соединены через **serial** кабель. Настройте протокол PPP с CHAP аутентификацией. Используйте подсеть 10.1.2.4/30.

12. Для маршрутизации между центральным и удаленным офисами используйте протокол EIGRP. ID маршрутизаторов должны быть первые два доступных адреса из подсети 10.1.1.0/25. Маршрутизаторы должны отправлять обновления только на необходимые для этого интерфейсы.

13. На внешнем интерфейсе маршрутизатора SM-PA-R1 настройте динамический nat с избытком используя два свободных адреса сети 80.1.128.0/28.

День 2. Настройка WINDOWS

1. На компьютере **VPC-PA** вы найдете предустановленную виртуальную машину **SM-WS1** с предустановленной Windows Server 2016.

2. Сделайте следующую базовую конфигурацию **SM-WS1**:

a. Раскладка клавиатуры по умолчанию 'US'.

b. Имя машины должно соответствовать схеме сети.

c. IP адрес сервера - 10.1.10.100/24.

d. Установите роль доменного контроллера:

i DNS имя домена **sunshine.local**, NetBIOS имя **sunshine**.

ii Режим леса должен быть максимально возможным.

iii DNS должен быть интегрированным с доменом.

e. Настройте переадресацию всех неизвестных запросов на адрес 192.168.10.100.

f. Настройте автоконфигурацию адресов для всех клиентов в домене:

i. Домен: **sunshine.local**; DNS Сервер: 10.1.10.100 и 10.2.10.100; WINS: -; Название зоны: **Par_Network**; Первый IP: 10.1.20.90; Последний IP: 10.1.20.99; Шлюз по-умолчанию: 10.1.20.254; Маска: 255.255.255.0; IPv6 DHCP: выключен.

ii. Домен: **sunshine.local**; DNS Сервер: 10.1.10.100 и 10.2.10.100; WINS: -; Название зоны: **Lil_Network**; Первый IP: 10.2.20.90; Последний IP: 10.2.20.99; Шлюз по-умолчанию: 10.2.20.254; Маска: 255.255.255.0; IPv6 DHCP: выключен.

iii. Компьютеры клиентов должны получать адрес с центрального DHCP сервера **SM-WS1**.

h. Создайте данные подразделения в домене:

Corp

Corp\Office

Corp\Sales

Corp\ITAdmin

PC

i. Компьютеры, которые в дальнейшем будут добавляться в домен, должны автоматически располагаться в подразделении PC.

ж. Создайте **G_Office**, **G_ITAdmin** и **G_Sales** группы в соответствующих подразделениях.

з. Создайте общую папку **Homes**. Домашние директории пользователей должны располагаться в данной папке. Обеспечьте, чтобы пользователи имели доступ только к своему каталогу.

4. Все пользователи должны иметь доступ к домашней папке через сетевой диск с буквой **H**.

и. Создайте пользователей **sa_user1** и **sa_user2**. Пользователи не должны менять свой пароль и должны быть членами группы **G_Sales**.

л. В подразделении **ITAdmin** создайте пользователей: **Cisco**, **OpenSource**, **SMAdmin**. **SMAdmin** должен иметь права администратора и состоять в группе «Администраторы предприятия». **Cisco** и **OpenSource** должны быть членами группы **G_ITAdmin**.

м. Создайте пользователя **of_user**. Этот пользователь должен относиться к подразделению **Office**.

н. **sa_user2** пользователь может аутентифицироваться на компьютерах только между 8-00 и 14-00 с понедельника по субботу.

о. Групповые политики должны быть применены к определенным подразделениям:

i Имя GPO: **Office GPO** ограничение: не могут менять экран блокировки.

ii Имя GPO: **Sales GPO** политика: пользователи не могут менять реестр и не должны иметь доступ к командной строке.

iii Имя GPO: **Laptops** политика: Нет возможности менять рисунок на компьютерах.

iv Имя GPO: **Local admin** политика: члены группы **G_ITAdmin** должны быть членами локальной группы Администраторы на всех клиентах.

3. На **SM-WS1** установите центр сертификации.

a) Тип центра должен быть Enterprise Root CA.

b) Имя центра сертификации должно быть SunshineCA, корневой сертификат должен быть актуальным 10 лет.

4. Компьютер **VPC-PA** должен быть настроен в соответствии с инструкциями ниже:

a) Создайте пользователя **Admin** с паролем **Pa\$\$w0rd**.

b) IP адрес должен получаться клиентом автоматически.

c) Добавьте клиента в домен.

d) Переместите **VPC-PA** в подразделение **Office**.

5. На компьютере **VPC-LI** вы найдете предустановленную виртуальную машину **SM-WS2** с предустановленным Windows Server 2016. Настройте следующие базовые настройки на сервере **SM-WS2**:

- a) IP адрес - 10.2.10.100/24.
- b) Добавьте сервер в домен.

6. На компьютере **VPC-LI** вы найдете предустановленную виртуальную машину **SM-LI1**. Компьютер **VPC-LI** и **SM-LI1** IP адрес должны получать автоматически, а также их надо добавить в домен.

7. На обоих серверах вы можете создать второй жесткий диск. Создайте раздел на обоих дисках и назначьте букву **К**.

8. Install the Windows Server Backup service on both servers.

9. Настройте бэкап по времени:

1. Каждый день с 6:00 and 22:00 должен начинаться бэкап.
2. Делайте бэкап только папки C:\Users\.
3. Бэкапы хранятся на диске **К**.

День 3.

Сетевое задание

После запроса изменить инфраструктуру сети офиса **Webdemand**, группа инженеров вашей компании разработала новую схему сети. Настройте оборудование исходя из схемы сети и инструкций.

1. Настройте подключение сети на внешнем интерфейсе маршрутизатора **WD-PA-R1** согласно представленной топологии.

2. Для менеджмента вашей сети настройте на всех устройствах имена в соответствии со схемой сети.

3. Создайте пользователя **WAdmin** на всех устройствах для аутентификации по SSH (SSHv2) для домена **cisco.com**. Для авторизации пользователя через SSH на устройствах установите пароль **sm@ssh**. Пользователь должен обладать максимальными привилегиями. Для увеличения безопасности аутентификация по telnet должна быть невозможна.

4. На всех маршрутизаторах и коммутаторах задайте сообщение при аутентификации о невозможности неавторизованного доступа.

5. Будущая сеть подразумевает синхронизацию часов с сервером синхронизации времени настроенным на маршрутизаторе **SM-PA-R1**. Настройте синхронизацию на всех сетевых устройствах.

6. Сервера и клиентские машины должны быть логически разделены. Для этого создайте 3 VLAN в центральном офисе с номерами и именами указанными далее. Вы должны использовать инструкции группы инженеров.

a. VLAN 99, Management, Адрес подсети: 192.168.30.0/24
Порты назначенные **WD-PA-SW1**: Fa0/20-24

b. VLAN 10, Server, Адрес подсети: 192.168.10.0/24
Порты назначенные **WD-PA-SW1**: Fa0/2-9

c. VLAN 20, Workers, Адрес подсети: 192.168.20.0/24
Порты назначенные **WD-PA-SW1**: Fa0/10-19

7. Шлюз по умолчанию в созданных VLAN должен быть последний адрес сети.

8. Для удаленного подключения коммутатор должен иметь первый адрес в Management VLAN.

9. Компьютеры клиентов должны получать адрес с DHCP. Настройте оборудование таким образом, чтобы клиенты из VLAN Workers получали информацию с DHCP сервера

10. На внешнем интерфейсе необходимо настроить nat с избытком, используя внешний интерфейс маршрутизатора.

11. Сайт *www.webdemand.ru* должен быть доступен из внутренней сети предприятия, включая центральный офис.

Настройка LINUX

1. На компьютере **VPC-WD** вы найдете две виртуальные машины названные **WD-LS1** и **WD-LS2**. Установите на них **ОС Debian**, создайте пользователя **wdadmin**.

2. Назначьте на **WD-LS1** IP адрес 192.168.20.100/24. Данная машина должна быть настроена как DHCP сервер для VLAN 10 и 20.

a. Для 20 VLAN, первый доступный адрес 192.168.20.10, последний 192.168.20.19. маска 255.255.255.0, DNS сервер **WD-LS1**.

b. Для 10 VLAN, первый доступный адрес 192.168.10.10, последний 192.168.10.19. Маска 255.255.255.0, DNS сервер **WD-LS1**.

3. **WD-LS1** является DNS сервером для данной сети. Для внешнего обращения к сервисам компании используется DNS сервер ISP с адресом 85.20.12.100. Доменное имя компании **webdemand.corp**. Добавьте DNS записи для всех устройств данной сети.

4. На **WD-LS1** установите веб сервер Apache2 и настройте его, следуя инструкции:

- a. Сайт *www.webdemandX.ru (/www/html)* должен быть сайтом по умолчанию. Добавьте имя этого сайта в качестве записи DNS сервера.
- b. Домашняя страница сайта должна содержать запись: **Welcome to webdemand site!**

5. На компьютере **VPC-WD** вы найдете виртуальную машину с именем **WD-PC1**. **WD-PC1** является клиентом в данной сети. На клиенте уже установлена базовая операционная система Debian ваша задача установить графический интерфейс **Gnome**. Данные настройки должны быть выполнены при конфигурации клиента:

- a. Созданный пользователь во время установки **root** с паролем **toor**.
- b. Виртуальная машина **WD-PC1** должна получать адрес по DHCP.

6. На **WD-LS2** необходимо установить почтовый сервер **Thunderbird** и настроить его почтовым сервером по умолчанию с использованием протоколов IMAP и SMTP.

7. Создайте следующих пользователей на **WD-LS2**:
webadmin, admin, projectuser1, projectuser2.

8. Формат почтового адреса должен быть `username@webdemand.corp`. Клиентами почтового сервера должны быть все ранее созданные клиенты на сервере **WD-LS2**. Удостоверьтесь, что они могут посылать сообщения друг другу.

Установите на **WD-PC1** почтовый клиент **Icedove** и настройте почтовые ящики всех пользователей.