**Конкурсное задание** 

Компетенция

(Сетевое и системное администрирование 14-16)



## 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 1х дня**.

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.

**Количество часов на выполнение задания: 4ч.**

## 3. ЗАДАНИЕ

Сетевая часть

##

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 SM-LT1, 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.
4. Создайте пользователя SMadmin на всех устройствах для аутентификации по SSH (SSHv2) для домена cisco.com. 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.
	1. 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:** Fa0/1-9

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

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

1. В удаленном офисе вам также потребуется создать 3 VLAN, но адреса подсети меняются таким образом, что второй октет адреса изменяется на 2:
	1. VLAN 1000, Management, Адрес подсети: 10.2.1.128/25

Порты назначенные на **SM-PA-SW2:** Fa0/20-24

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

Порты назначенные на **SM-PA-SW2:** Fa0/1-9

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

Порты назначенные на **SM-PA-SW2:** Fa0/10-19

1. В обоих офисах шлюз по умолчанию в созданных VLAN должен быть последний адрес сети.
2. Для удаленного подключения коммутаторы должны иметь первый адрес в Management VLAN.
3. Два офиса соединены через serial кабель. Настройте протокол PPP с CHAP аутентификацией. Используйте подсеть 10.1.2.4/30.
4. 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.
5. Оба офиса должны получать через маршрутизатор SM-PA-R1. Настройте доступ с настройкой шлюза по умолчанию в сторону сети Интернет, и объявите это удаленному офису.
6. На внешнем интерфейсе маршрутизатора SM-PA-R1 настройте динамический nat с избытком используя два свободных адреса сети 80.1.128.0/28.

## Серверная часть

1. На компьютере SM-PC1 вы найдете предустановленную виртуальную машину SM-WS1 c предустановленный Windows Server 2016.
2. Сделайте следующую базовую конфигурацию **SM-WS1**:
	* + 1. Раскладка клавиатуры по умолчанию 'US'.
			2. Имя машины должно соответствовать схеме сети.
			3. IP адрес сервера - 10.1.10.100/24.
			4. Установите роль доменного контроллера.
				1. DNS имя домена **sunshine.local,** NetBIOS имя **sunshine.**
				2. Режим леса должен быть максимально возможным.
				3. DNS должен быть интегрированным с доменом.

e. Настройте переадресацию всех неизвестных запросов на адрес 192.168.10.100.

* + - 1. Настройте автоконфигурацию адресов для всех клиентов в домене
		1. 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.
		2. 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.
		3. Компьютеры клиентов должны получать адрес с центрального DHCP сервера SM-WS1. Настройте оборудование таким образом, чтобы клиенты из VLAN Workers получали информацию с DHCP сервера.
		4. Создайте данные подразделения в домене:

Corp

Corp\Office

Corp\Sales

Corp\ITAdmin

PC

* + 1. Компьютеры, которые в дальнейшем будут добавляться в домен должны автоматические располагаться в подразделении PC.
		2. Создайте **G\_Office**, **G\_ITAdmin** и **G\_Sales** группы в соответствующих подразделениях.
		3. 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:.
1. Создайте пользователей sa\_user1 и sa\_user2. Пользователи не должны менять свой пароль и должны быть членами группы G\_Sales.
2. 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** .
3. Создайте пользователя **of\_user**. Этот пользователь должен относиться к подразделению **Office.**
4. **sa\_user2** пользователь может аутентифицироваться на компьютерах только между 8-00 и 14-00 с понедельника по субботу.
5. Групповые политики должны быть применены к определенным подразделениям:
	1. Имя GPO: **Office GPO**; ограничение: не могут менять экран блокировки.
	2. Имя GPO: **Sales GPO** политика: пользователи не могут менять реестр и не должны иметь доступ к командной строке.
	3. Имя GPO: **Laptops** политика: Нет возможности менять рисунок на компьютерах.
	4. Имя GPO: **Local admin** политика: члены группы **G\_ITAdmin** должны быть членами локальной группы Администраторы на всех клиентах.
6. На **SM-WS1** установите центр сертификации.
	1. Тип центра должен быть Enterprise Root CA.
	2. Имя центра сертификации должно быть SunshineCA, корневой сертификат должен быть актуальным 10 лет.
7. Компьютер **SM-PC1** должен быть настроен в соответствии с инструкциями ниже:
	* 1. Создайте пользователя **Admin** с паролем **Pa$$w0rd**.
		2. IP адрес должен получаться клиентом автоматически.
		3. Добавьте клиента в домен.
		4. Переместите **SM-PC1** в подразделение **Office**.
8. На компьютере SM-LT1 вы найдете предустановленную виртуальную машину **SM-WS2** c предустановленным Windows Server 2016. Настройте следующие базовые настройки на сервере **SM-WS2**:
	* + 1. IP адрес - 10.2.10.100/24.
			2. Добавьте сервер в домен.
9. На компьтере **SM-LT1** должны быть сделаны следующие настройки:
	* + 1. IP адрес должен получаться клиентом автоматически.
			2. Добавьте клиента в домен.
10. На обоих серверах вы можете создать второй жесткий диск. Создайте раздел на обоих дисках и назначьте букву K:.
11. Install the Windows Server Backup service on both servers.
12. 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 K: .

**Топология сети**

