	Проект конкурсного задания
39	ИТ Сетевое и системное администрирование

Введение

Название профессиональной компетенции: Сетевое и системное администрирование.

Описание профессиональной компетенции.

Сетевое и системное администрирование требует широких познаний в области информационных технологий. В связи с быстрым развитием этой области, требования к администраторам постоянно возрастают. Системный и сетевой администратор (инженер) должен уметь:

- Разрабатывать и развертывать комплексную информационную инфраструктуру предприятий, включающую рабочие станции, серверы и сетевое оборудование, сетевое оборудование.
- Развертывать основные сервисы, включая службы каталогов, резервного копирования, почтовые и другие прикладные сервисы.
- Использовать широкий набор операционных систем и серверного ПО.
- Эффективно организовывать защищенные соединения сетей предприятий, доступ в Интернет и иные сети.
- Устанавливать и настраивать устройства беспроводной сети, коммутаторы, маршрутизаторы и средства защиты информации.
- Организовывать защиту информации от несанкционированного доступа.
- Разрабатывать документацию информационной структуры предприятия.
- Устанавливать, настраивать и отлаживать программные и аппаратные средства VoIP.

• Устанавливать и настраивать сетевые сервисы на базе протоколов IPv4 и IPv6.

• Устанавливать, настраивать и поддерживать виртуальные среды.

• Осуществлять поиск и устранение неисправностей в работе информационных систем и сетей.

Форма участия в конкурсе

Индивидуальный конкурс.

Модули задания и необходимое время

Модули и время сведены в таблице 1

Таблица 1.

№ п/п	Наименование модуля	Рабоче время	Время на задание
1	Модуль 1: День 1. Сетевые технологии	С1 09.00-12.00 С1 13.00-15.00	3 часа 2 часа
2	Модуль 2: День 2. Работа с ОС Microsoft Windows	С1 09.00-12.00 С1 13.00-15.00	3 часа 2 часа
3	Модуль 3: День 3. Работа с ОС Linux CentOS	С1 09.00-12.00 С1 13.00-15.00	3 часа 2 часа

Модули задания и необходимое время

В данном разделе определены критерии оценки и количество начисляемых баллов (субъективные и объективные) таблица 2. Общее количество баллов задания/модуля по всем критериям оценки составляет 100.

Таблица 2.

Раздел	Критерий	Оценки		
		Субъективная (в режиме судейства)	Объективная	Общая
A	Модуль 1: День 1. Сетевые технологии	3	31	34
B	Модуль 2: День 2. Работа с ОС Microsoft Windows	0	33	33
C	Модуль 3: День 3. Работа с ОС Linux CentOS	0	33	33
	Итого:	3	97	100

Субъективная оценка относится к выполнению участником задания, связанного с ведением технической документации и планированием работ.

Субъективная оценка выполняется в режиме судейства (Judgment), где судьи выставляют свои оценки исходя из следующих соображений:

0 - нечего оценивать. Документ отсутствует или не является реализуемой (содержит грубые ошибки).
1 - Документ не конкретен, может трактоваться различными способами, допускает разные варианты реализации.
2 - Документ однозначен и реализуем, но содержит недочеты.
3 - Все выполнено идеально.

Конкурсное задание

Общая информация

Мы рады приветствовать вас, в нашем дружном коллективе, наша компания, в которую вы только что устроились, занимается IT аутсорсингом. И вашими обязанностями будет работа с IT-инфраструктурой наших клиентов. Одним из них является торгово-строительная компания «Айперф», которая провела успешную сделку по покупке бизнеса своего конкурента «СтройСеть». На текущий момент вашей основной задачей является обеспечить слияние IT-инфраструктуры этих организаций.

К сожалению «СтройСеть» не является нашим клиентом, и его инфраструктура, в условиях жестокой экономии, находится в плачевном состоянии и принято решение построить все с нуля. Также руководство «Айперф», в связи с расширением бизнеса планирует произвести значительную модернизацию своей сети. Поэтому задача перед вами стоит трудоемкая и ответственная, но с вашим опытом и квалификацией о которой вы рассказали нам на собеседовании, эта задача вполне вам по силам.

Вам будут предоставлены вся документация по сети нашего клиента «Айперф», а также та информация, что имеется по сети «СтройСеть».

Сейчас каждый час на счету, а потому наше руководство требует, чтобы через 3 дня все задачи по объединению ИТ-систем компаний были выполнены.

День 1. Сетевые технологии

Сегодня вам предстоит много работы. Сначала необходимо внести серьезные изменения в инфраструктуру сети «Айперф», затем – в соответствии с выбранным дизайном обеспечить создание инфраструктуры «СтройСеть».

1. Используя предоставленные документы, формы и схемы, необходимо подключить все устройства сети.

В сети компании «Айперф» за маршрутизацию между VLAN отвечает коммутатор 3ого уровня SW1.

2. Подключите порт F0/1 маршрутизатора R1 к порту F0/1 коммутатора SW1.
3. Переключите порт F0/1 коммутатора SW1 в маршрутизируемый порт.
4. На SW1 включите маршрутизацию IPv4.
5. Настройте IP-адресацию устройств в соответствии с утвержденной схемой.

В соответствии с дизайном будущей сети, нам необходимо настроить протокол динамической маршрутизации, который позволит обмениваться маршрутами между SW1, R1 и R2.

6. Настройте OSPF между SW1 и R1, используя аутентификацию MD5.
7. Отключите отправку информации о маршрутах на всех интерфейсах кроме F0/1 на SW1 и F0/0, F0/1 на R1.

Маршрутизатор R1 предполагается использовать как IP-телефонную станцию.

8. Запустите на R1 сервис IP телефонии.
9. В качестве тестового телефонного аппарата подключите к телефонной сети софтфон Cisco IP Communicator на PC1, дистрибутив которого есть

в вашем комплекте ПО. Софтфон должен зарегистрироваться и получить номер 10001.

После того как закончите с сетью «Айперф», переходите к сети «СтройСеть», после подключения всех устройств, и их настройки. Вам необходимо будет организовать защищённый IPsec туннель до сети «Айперф». Который необходим:

- Для обмена информацией между узлами и серверами сетей обоих компаний.

- Для подключения телефонных аппаратов «СтройСеть» к станции IP-телефонии «Айперф».

- Для передачи интернет трафика узлов сети «СтройСеть».

В сети компании «СтройСеть» используется коммутатор 2ого уровня, и маршрутизацию между VLAN обеспечивает маршрутизатор R2, который настроен по схеме «router on a stick».

10. Подключите порт F0/1 SW2 к порту F0/1 R2.
11. Подключите порт F0/0 R1 к порту F0/0 R2.
12. На коммутаторе SW2 создайте сети VLAN в соответствии со схемой.
13. Настройте схему «router on a stick» между R2 и SW2.
14. К порту F0/24 SW2 подключите IP телефон.
15. Порт F0/24 SW настройте в режиме доступа на VLAN10 для подключения PC2 к сети предприятия, а также добавьте «Voce VLAN», для подключения IP-телефона в отдельном VLAN к IP-сервису R1

Далее необходимо настроить безопасный канал между сетями предприятий. Как мы говорили ранее, необходимо использовать протокол IPsec.

16. Между маршрутизаторами R1 и R2 должен быть настроен статический IPsec-туннель. Параметры защиты данных описаны в Политике информационной безопасности компании. Этот туннель должен защищать весь трафик.

17. Пользовательские компьютеры компании «СтройСеть» должны получать все необходимые параметры от DHCP-сервера, который должен быть настроен на R1, R2 должен выполнять функции DHCP-relay.

18. Настройте динамическую маршрутизацию OSPF на R2, для того, чтобы он мог обмениваться маршрутами с R1 и SW1.

19. Отключите пересылку обновлений маршрутизации на неиспользуемые порты.

Нужно обеспечить работу IP-телефонии. Необходимое оборудование у вас имеется, но его нужно подключить и настроить.

20. Обеспечьте подключение нового оборудования в соответствии с утвержденной таблицей соединений и подключений. Настройте R2 так, чтобы все необходимые параметры для работы телефонии выдавались устройству автоматически по протоколу DHCP.
21. Настройте R1 так, чтобы новое устройство могло зарегистрироваться в системе с телефонным номером 10101. Убедитесь, что звонок на номер 10001 проходит и обе стороны слышат друг друга.

День 2. Работа с ОС Microsoft Windows

Доброе утро коллега. Вчерашний день выдался не легким. Хотя настройка сетевого оборудования уже позади, впереди еще много работы.
Ключевыми задачами, решаемыми любой инфраструктурой, является контролируемый доступ пользователей к данным.
В первую очередь необходимо будет установить и настроить новый сервер, который будет выполнять роль хоста виртуальных машин под управлением Microsoft Hyper-V.

1. Необходимо установить Windows Server 2012 R2 на HOST_VM.
2. На HOST_VM настроить Microsoft Hyper-V.

3. Установить вириальную машину SrvAD под управлением Windows Server 2012 R2.
4. Добавить на сервер SrvAD следующие роли: контроллера домена, файловый сервер и dns сервер.
5. Имя домена использовать iperf.local.
6. В домене создать группу usriperf и добиться, чтобы к ее членам применялась гранулярная политика усиленной безопасности, в частности ее опция повышенной сложности паролей.
7. Для файлового сервера выделить директорию C:\files\iperf и дать к ней полный доступ группе пользователей usriperf.
8. Подключить к установленному контроллеру домена персональные компьютеры пользователей обоих сетей.

День 3. Работа с ОС Linux CentOS

И снова доброе утро, коллега. Сегодня вам предстоит завершающий этап кропотливой работы. И для этого необходимо разобраться с оставшейся инфраструктурой.
Начнем с установки Linux серверов на хост виртуальных машин HOST_VM.

9. В Hyper-V необходимо создать виртуальную машину и установить на нее операционную систему CentOS, настроить на нем службу FTP сервера.
10. На второй сервер под управлением CentOS должна быть установления служба Web-сервера Apache+PHP.
11. На веб сервере создать страницу сайта, которая должна быть доступна по HTTP и иметь содержание в виде названия компании «Айперф», а также текущую дату и время.
12. Третий сервер под управлением CentOS должен являться radius сервером.
13. Radius сервер должен использоваться для аутентификации и авторизации на сетевые устройства SW1, SW2, R1 и R2 по системе AAA.

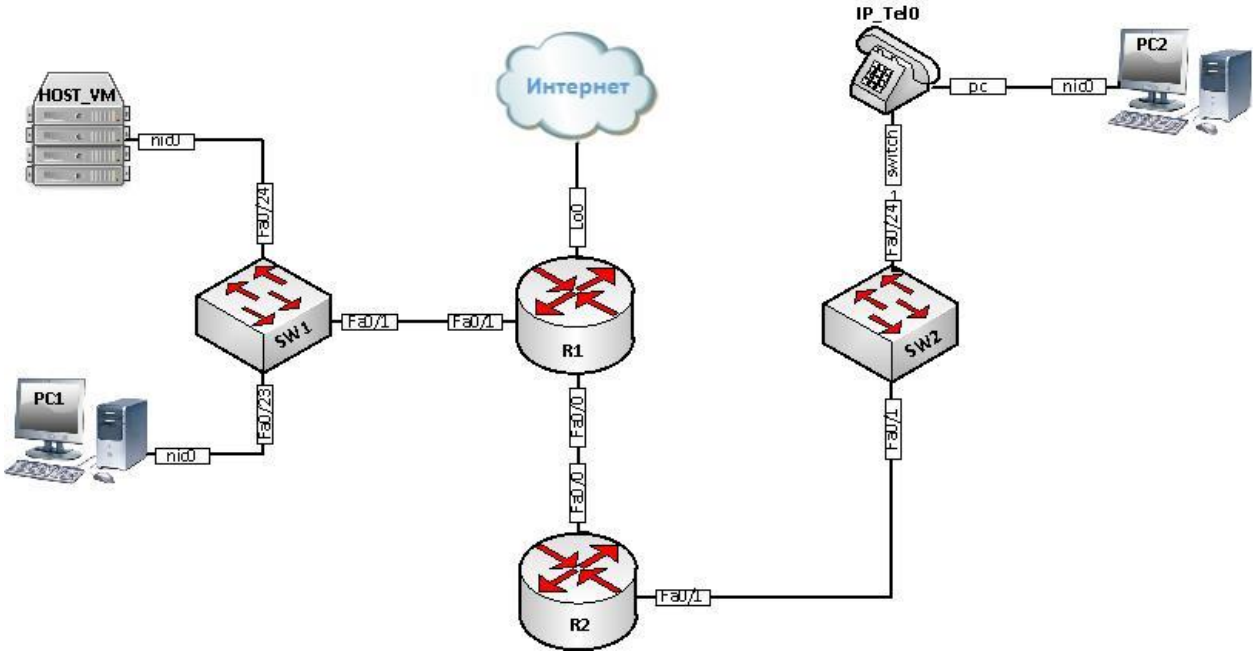
Приложение 1. Политика безопасности «Айперф» в области информационных технологий и защиты информации

1. Вся информация, хранимая, передаваемая и обрабатываемая с использованием вычислительных средств корпорации «Айперф», является собственностью корпорации. Руководство компании имеет неограниченный доступ к информации. Доступ прочих сотрудников к информации определяется действующими регламентами и распоряжениями руководства.
2. В корпоративной сети используется диапазон адресов 10.0.0.0/16. Все устройства в сети, если это не указано явно, должны иметь адреса из указанного диапазона. Каждое подразделение должно иметь собственный диапазон адресов с маской 255.255.255.0. Транзитные сети (предназначенные для обеспечения связи между маршрутизаторами) должны иметь адреса из диапазона 10.0.255.128/25 и максимальную длину маски, достаточную для обеспечения связи. Использование маски /31 категорически запрещено, использование маски /32 допускается только для адресации Loopback-интерфейсов.
3. Все маршрутизаторы должны иметь интерфейс Loopback 0 с адресом в формате 10.0.255.z/32 из диапазона 10.0.255.0/25. Выделение адресов производится по возрастанию.
4. Все сетевые устройства должны синхронизировать свои часы с часами контроллера домена. Журнальная информация с сетевых устройств должна передаваться на специализированный syslog-сервер. Перед проведением работ, связанных с изменением конфигураций, критическая информация должна быть сохранена на TFTP-сервер. По окончании работ финальные конфигурации также должны сохраняться.
5. Телефонная связь внутри корпорации осуществляется по технологиям IP-телефонии. Звонки между филиалами и центральным офисом в обязательном порядке должны шифроваться.
6. Шифрование телефонных звонков между филиалами, а также шифрование всего прочего трафика не обязательно, но допускается.

7. При использовании шифрования трафика применяются IPSec-туннели со следующими характеристиками:
    - Аутентификация – по общему ключу
    - Шифрование – 3DES или более стойкое
    - Контроль целостности – SHA1 или более стойкий
8. Допускается совмещение функций IP-телефонного шлюза и криптошлюза на одном устройстве.
9. Внутри сети корпорации используется протокол динамической маршрутизации OSPF. Сеть головного офиса включается в Backbone Area (Area 0).
10. Удаленный доступ к интерфейсам управления разрешается только в случае использования защищенных протоколов передачи данных, поддерживающих как аутентификацию, так и шифрование данных.
11. Получать доступ для управления сетевыми устройствами могут получать только пользователи из головной организации.
12. Для всех используемых веб-серверов на платформе ОС Linux должна соблюдаться следующая парольная политика:

- пароль должен состоять из символов принадлежащих как минимум трем множествам (например, верхний и нижний регистр, цифры);
- длина пароля не должна быть меньше 8 символов;
- рядовой пользователь не может создать пароль, противоречащий заданным правилам; администратор может, но должен получать предупреждение;
- пользователи не должны входить в системную консоль как администраторы, но должны иметь возможность переключаться в контекст суперпользователя, используя команду su;

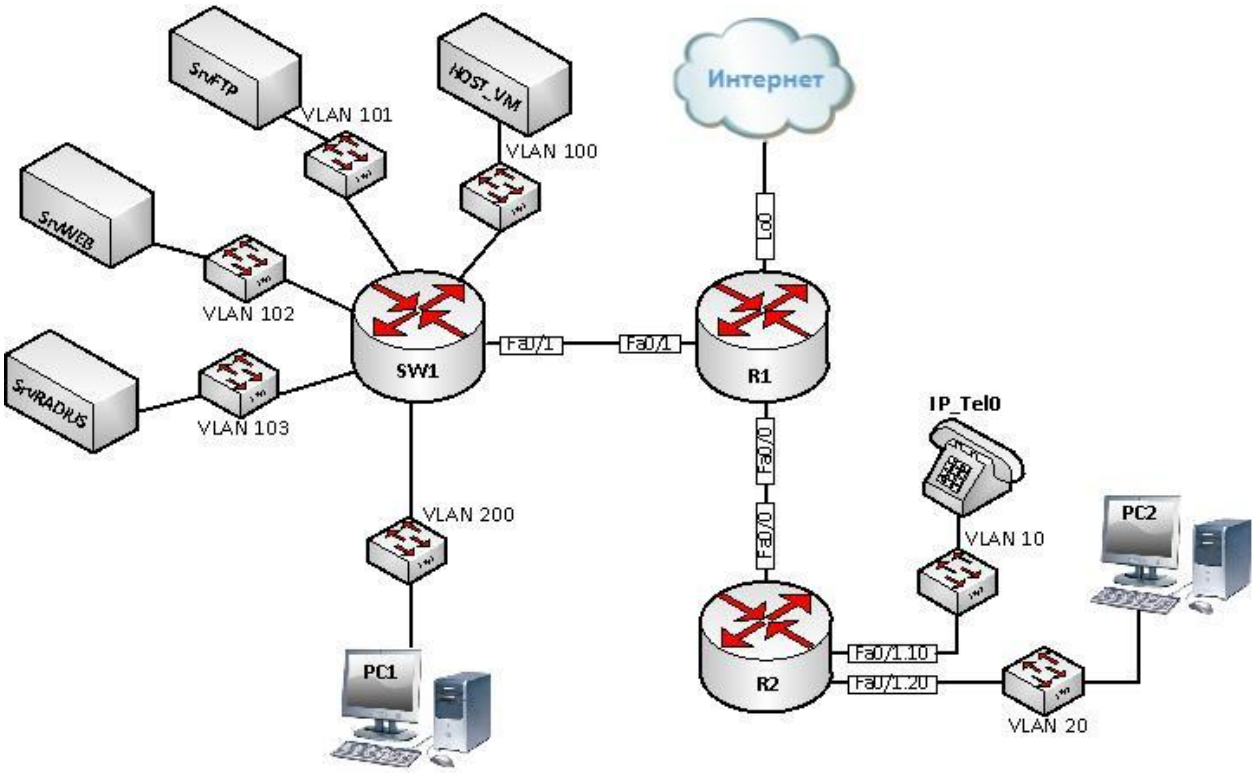
Приложение 2. Схема соединений и подключений (физический уровень)



Приложение 3. Таблица соединений и подключений

SW1	Устройство	Порт	SW2	Устройство	Порт	R1	Устройство	Порт	R2	Устройство	Порт	IP_Tel0	Устройство	Порт
F0/1	R1	F0/1	F0/1	R2	F0/1	F0/0	R2	F0/0	F0/0	R1	F0/0	Switch	SW2	F0/24
F0/2			F0/2			F0/1	SW1	F0/1	F0/1	SW2	F0/1	PC	PC2	NIC0
F0/3			F0/3			S0/1/0			S0/1/0					
F0/4			F0/4			S0/1/1			S0/1/1					
F0/5			F0/5											
F0/6			F0/6											
F0/7			F0/7											
F0/8			F0/8											
F0/9			F0/9											
F0/10			F0/10											
F0/11			F0/11											
F0/12			F0/12											
F0/13			F0/13											
F0/14			F0/14											
F0/15			F0/15											
F0/16			F0/16											
F0/17			F0/17											
F0/18			F0/18											
F0/19			F0/19											
F0/20			F0/20											
F0/21			F0/21											
F0/22			F0/22											
F0/23	PC1	NIC0	F0/23											
F0/24	HOST_VM	NIC0	F0/24	IP_Tel0	Switch									
G0/1														
G0/2														

Приложение 4. Схема соединений и подключений (канальный уровень)



Приложение 4. Схема соединений и подключений (Сетевой уровень)