Конкурсный день 1.

Год 2016. Вас как специалиста в сфере ИТ пригласила на работу крупная дистрибьюторская компании «Company». Компания «Company» занимается продажей шоколада на территории Российской Федерации, входит в TOP-10 производителей и дистрибьюторов шоколада в стране, имеет разветвленную филиальную инфраструктуру во всех, даже самых отдаленных уголках нашей Родины. Штаб-квартира компании, кодовое название ЦО, сегодня переезжает в новый офис. Вам, как нашему новому системному инженеру, необходимо развернуть за один день информационную инфраструктуру ЦО.

Создание ЛВС ЦО:

1. Обжать два коммутационных шнура для подключения коммутатора к маршрутизатору и для подключения сервера к коммутатору.
2. Подключить порт F0/0 маршрутизатора к порту F0/24 коммутатора.
3. Подключить сервер к порту F0/1 коммутатора.
4. Известно, что маршрутизатор переехал из старого офиса компании и уже частично преднастроен. Известно, что IP-адрес маршрутизатора 10.0.252.254, он настроен на подинтерфейсе в Виртуальной ЛВС (ВЛВС) 252, и эта ВЛВС не тэгируемая. Логин\пароль - cisco\cisco.
5. Известно, что коммутатор также переехал из старого офиса компании. А в старом офисе ВЛВС 252 использовали в качестве сети управления сетевым оборудованием и серверами. IP-адрес коммутатора 10.0.252.100.

Связь с филиалами:

Ближайший к вам филиал - один из старейших филиалов компании, офис «Северный». Необходимо восстановить с ним связь. Логин для доступа - cisco. Чтобы не указывать пароль от маршрутизатора в документации в открытом виде, служба безопасности ЦО решила записать его в виде формулы пароль=cisco + OSPF_Metric_for(T1 line). *Пароль выглядит как ciscoXXXX, где XXXX - это численное значение метрики.*

Проверьте, что ЛВС филиала «Северный» настроена согласно документации, хранящейся в архиве компании. Филиал подключен к глобальной сети Интернет. Поэтому для защиты конфиденциальной информации мы решили использовать технологию VTP. Однако необходимо обеспечить работу динамических протоколов маршрутизации через данное подключение, поскольку филиал «Северный» является транзитным узлом для подключения других филиалов компании. Если для решения данной задачи вам необходимы IP-адреса, используйте 10.255.255.0/24. *Передавать любую информацию по открытому каналу связи между ЦО и филиалом «Северный» - **запрещено!!!** Сконфигурируйте соответствующие списки контроля доступа.*

В качестве протокола динамической маршрутизации используйте OSPF. На всех линиях связи, где устанавливаются соседские отношения OSPF, используйте пароль CiscoCisco для защиты OSPF-пакетов. Используйте самый надежный метод защиты. Необходимо обеспечить связь ЛВС всех филиалов и ЛВС ЦО. Для оптимизации размера таблиц маршрутизации используйте ***суммаризацию***.

Конкурсный день 2.

На сервер ЦО уже установлена ОС MS Win 8.1. Установите Vmware Workstation.

1. Создать ВМ dc01 – установить ОС Win Server 2012, назвать сервер dc01, настроить сетевые параметры согласно **таб.1**, настроить роль контроллера домена и DNS для домена Company.ru.

Ввести в домен «Company».ru компьютер comp-so из филиала «Северный».

Создать организационные единицы, группы и пользователей в домене Company.ru в соответствии с **таб. 3.**

Настройте сайты AD в соответствующих подсетях.

2. Создать ВМ term01 – установить ОС Win Server 2012, назвать сервер ВМ term01, настроить сетевые параметры согласно **таб.1**, ввести в домен Company.ru.

- Разверните терминальный сервер с лицензированием по компьютерам (используйте временную лицензию);
- Сконфигурируйте веб доступ RemoteApp к службам терминалов сервера;
- Опубликуйте программу «WordPad» на веб-портале RemoteApp для всех сотрудников отдела ИТ «Северный»;
- Создайте политику распространения пакета «RemApp_PT» для всех входящих в группу «SO_IT» в филиале «Северный».

3. Установите почтовый сервер hMailServer (дистрибутив на флеш-накопителе) на сервер term01. Создайте почтовые ящики пользователей ЦО в формате UserX в домене Company.ru (**таб. 3**).

4. Создать сетевые папки в соответствии с **таб. 4** на сервере term01. Настроить фильтры блокировки файлов (запретить хранение исполняемых файлов, системных файлов, файлов аудио и видео) **таб. 5**.

5. Имея в своем распоряжении такой мощный инструмент как AD, мы просто обязаны им воспользоваться для повышения уровня автоматизации и контроля за ИС нашей организации. Настройте и примените групповые политики к пользователям и клиентским рабочим станциям домена:

- Для того чтобы всем пользователям в нашей организации привить стремление к сохранности корпоративных данных, ужесточим некоторые политики безопасности. Создайте политику учетных записей для всех пользователей домена Company.ru в соответствии с **таб. 6**;
- В нашей организации постоянно думают о том, как повысить удобство пользования внутренними сервисами для сотрудников компании, а также о том, как увеличить эффективность и уровень безопасности, поэтому неплохо было бы предоставить возможность запускать каждому пользователю в зависимости от его задач только необходимый ему набор ПО на терминальном сервере, прямо из меню Пуск его компьютера. Разверните средствами групповой политики домена пакеты MSI удаленных приложений RemoteApp на компьютерах пользователей (WordPad для пользователей Отдела ИТ в филиале «Северный» (SO_IT);
- Системные администраторы нашей организации прямо заинтересованы в том, чтобы иметь возможность полноценно управлять всеми компьютерами пользователей в домене. При

помощи групповых политик домена добавьте пользователей отдела «ЦО/Отдел ИТ» в локальную группу администраторов для всех компьютеров (ноутбуков) домена Company.ru (IT_Rest_Group);

- Для того чтобы наши сотрудники смогли наконец начать пользоваться нашим файловым сервером, необходимо подключить для них сетевые диски. При помощи групповых политик домена подключите сетевые папки с файлового сервера как диски (Net_Share_Sales - сетевую папку \\term01.Company.ru\docs_Sales как диск E: для сотрудников всех отделов продаж, входящих в домен Company.ru
- Наша служба поддержки не очень любит выезжать в филиалы и решает проблемы пользователей по телефону. При помощи групповых политик домена включите удаленный рабочий стол на всех компьютерах, находящихся в данный момент в филиале «Северный» (RDP_ON);
- Корпоративный стиль в нашей компании должен сохраняться во всем. При помощи групповых политик домена запретите «Корзину» на рабочем столе, запретите менять тему и рисунок рабочего стола, отключите экранную заставку для всех пользователей домена Company.ru.

Конкурсный день 3.

Год 2017. Когда-то давно, так давно, что уже никто и не помнит, Компания «Company» купила себе филиал в одном отдаленном уголке нашей родины**.** Филиал располагался в бывшем здании колхоза «Южный», поэтому решили филиал не переименовывать и оставить старинное название - филиал «Южный». Город был провинциальным вдоль и поперек, что наложило свой отпечаток на жизнь людей и сопутствующую инфраструктуру. Доступа в Интернет, как и сотовой связи, в городе не было, а из средств коммуникаций в местном почтовом отделении работали старенькая АТС, да трофейный коммутатор Frame Relay. Собственно, через Frame Relay и была организована связь с ЦО.

Канал Frame Relay был очень низкоскоростной, следовательно, ни о каких корпоративных сервисах через VPN не могло быть и речи. Все основные сервисы организовали локально – в филиале был установлен ПК с гордым названием «Сервер Южный», который отвечал за электронную почту и исполнял роль контроллера домена. Стоит отметить, что каждый четверг в 11 утра генеральный директор «Company» проводит плановое совещание посредством телефонной связи. В прошлый четверг филиал «Южный» не вышел на связь, и уже неделю из филиала нет отчетов по электронной почте. Финансовый квартал подходит к концу, и мы бы хотели получить финансовые показатели с периферии. Вам, как нашему главному «полевому» инженеру, необходимо отправится в филиал «Южный» и обеспечить сдачу квартальной отчетности, одновременно восстановив телефонную связь филиала.

Вы прибыли в филиал «Южный». Да… Печальное зрелище: коммутационный шнур между коммутатором и рабочим ПК поврежден ударом топора, а сетевой кабель между сервером и коммутатором исчез и, кажется, используется в качестве бельевой веревки в соседнем доме. Хорошо, что коммутационное оборудование на месте – закрыто в несгораемом сейфе директора филиала. Директора нигде нет. Что ж, приступим к восстановительным работам.

Прежде всего – восстановите СКС. Обожмите коммутационные шнуры для подключения коммутатора, ноутбука, маршрутизатора; обожмите сетевой кабель для подключения сервера к коммутатору. Поскольку старый сервер бесследно пропал, придется использовать в качестве нового сервера обычный ПК секретаря.

Отлично, СКС восстановлена, новый сервер подключен. Попробуем выяснить, почему же нет связи с ЦО. Из скудной документации по данному филиалу известно, что:

1. На портах коммутатора настроена функция PortSecurity. Коммутатор с маршрутизатором заперты в сейфе. Порт подключения сервера, похоже что, отключен.
2. Ноутбук директора точно такой же, как и у вас. Значит, MAC-адреса должны совпадать, если они из одной партии, то можно попробовать перебрать всего 16 значений в последних 4-х битах адреса (MAC партии нотубуков 0000.C1C0.CCC**X**).
3. Чтобы не указывать пароль от коммутатора в документации в открытом виде, служба безопасности ЦО решила записать его в виде дополнительного кода 9ABC для получения пароля необходимо перевести дополнительный код в десятичную систему счисления. (Логин - **cisco**, пароль от enable - **cisco**)
4. *Конечно, вы всегда сможете взломать сейф и сбросить пароль с коммутатора и маршрутизатора. Но порча казенного имущества займет много времени и обернется для вас потерей половины баллов за день.*

Отлично, вы попали на коммутатор, и теперь легко решите проблему связи с маршрутизатором. Не так ли? Ведь осталось всего лишь попасть на маршрутизатор, и можно будет восстановить связь и быстрее уехать домой.

Пароль от маршрутизатора безвозвратно утрачен и консольного кабеля у вас нет, так что выполнить процедуру восстановления пароля на маршрутизаторе не получится... Придется применить хакерские навыки и взломать пароль с помощью брутфорса – к счастью, на флешке есть папка с необходимым ПО и словарями, а имя пользователя, как обычно, **cisco**.

После того, как вы попали на маршрутизатор, осталось совсем немного – восстановить связь с ЦО и настроить\проверить IP-телефонию.

Для связи с ЦО используется старенькая линия Frame Relay. Единственная оставшаяся документация по ней - это древняя схема подключения филиала «Южный» к ЦО. Настройте связь между маршрутизаторами филиалов «Южный» и «Северный» через Frame Relay. При настройке Frame Relay используйте только физические интерфейсы и минимальное количество команд. После настройки Frame Ralay необходимо настроить маршрутизацию между филиалами «Северный» и «Южный». Используем протокол OSPF. **Нельзя менять тип OSPF сети на Frame Relay интерфейсах.**

Для сервера придётся использовать ПК секретаря директора. К счастью, ничего тяжелого запускать на сервере не нужно – для восстановления нормальной работы филиала необходимо восстановить только почтовый сервер на базе ОС Linux. Кажется, у вас где-то были установочные диски…

Почтовый сервер.

1. Установить ОС Debian на сервер. Установить и настроить почтовый сервер Sendmail (включая DoveCot IMAPd). В качестве DNS использовать сервер dc01. **Известно, что IP почтового сервера в ЦО – 10.0.252.3, а имя почтового домена филиала «Южный» - south.Company.ru**
2. Настроить почтовые ящики в виде UserX в почтовом домене south.Company.ru(**таб. 3**).
3. Обеспечьте маршрутизацию почтовых сообщений между филиалом «Южный» и ЦО.
4. Сотрудники филиала «Южный» привыкли работать с почтой через WEB-интерфейс. Наверняка, ОС Debian поставляется со всем необходимым ПО. *Для проверки работы почтовой службы установите ПО Mozilla Thunderbird на ноутбук comp_so филиала «Северный». В филилале «Южный» используйте WEB-браузер на ноутбуке для отправки почтового сообщения сотруднику в филиале «Северный».*

Таблица 1.

ВМ\Сервер	**Параметры ВМ**	**ОС**	**Сетевая конфигурация**
Mail50.south.Company.ru	1 vCPU 1 ГБ RAM 60ГБ HDD 1 vNIC	Debian Linux	IP:192.168.203.2 Mask:255.255.255.0 GW:192.168.203.254
dc01.Company.ru	2 vCPU 2 ГБ RAM 100 ГБ HDD 1 vNIC	Windows Server 2012	IP:10.0.252.2 Mask:255.255.255.0 GW:10.0.252.254
term01.Company.ru	2 vCPU 3 ГБ RAM 100 ГБ HDD 1 vNIC	Windows Server 2012	IP:10.0.252.3 Mask:255.255.255.0 GW:10.0.252.254 DNS:10.0.252.2

Таблица 2.

Ноутбук	**ОС**	**Сетевая конфигурация**
comp_ug	Windows 8.1	IP: 192.168.203.3 Mask: 255.255.255.0 GW: 192.168.203.254 DNS: 10.0.252.2
comp_so	Windows 8.1	IP: 192.168.225.1 Mask: 255.255.255.0 GW: 192.168.225.254 DNS: 10.0.252.2

Таблица 3.

Домен	**Уч. запись**	**Организац. ед.**	**ФИО**	**Член групп**
Company.ru	admin	ЦО/Админы	Дмитрий Алексеев	Administrators Domain admins Enterprise Admins
Company.ru	User1	ЦО/Отдел	Ирина	Domain Users

		продаж	Алексеева	CO_Sales
Company.ru	User2	ЦО/Менеджеры	Александр Макашев	Domain Users CO_Managers
Company.ru	User3	Север/Отдел ИТ	Илья Петров	Domain Users SO_IT
Company.ru	User4	Север/Отдел продаж	Андрей Бабич	Domain Users SO_Sales
Почтовый домен south.Company.ru	User6		Андрей Муллин	
Почтовый домен south.Company.ru	User7		Кирил Игошев	

Таблица 4.

Путь к папке	**Сетевой путь**
C:\Folders\docs_Sales	\\term01.Company.ru\docs_Sales
C:\Folders\IT	\\term01.Company.ru\IT$
C:\Folders\Manager	\\term01.Company.ru\docs_manager

Таблица 5.

Папка	**Группы файлов для блокировки**	**Квотирование**
C:\Folders\docs_Sales	Исполняемые файлы; Системные файлы; Файлы аудио и видео;	Жесткая квота Порог: 150МБ с расширением 50Мб
C:\Folders\IT	Нет	Нет

Таблица 6.

Атрибут	**Значение**
Вести журнал паролей	8
Максимальный срок действия пароля	31
Пароль должен отвечать требованиям сложности	включено
Минимальная длина пароля	8

Продолжительность блокировки учетной записи	5
Пороговое значение блокировки	3
Время до сброса счетчика блокировки	5