

**КОНКУРСНОЕ ЗАДАНИЕ  
ПО  
IT СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ**

**VOLOGDA 2016**

## **Компетенция «Сетевое и системное администрирование»**

### **Первый день**

Соревнование длится 12 часов, по 6 часов на каждый день соревнований. Вы должны правильно распределить время и силы для решения задания. Для более полного понимания задания и удачного распределения времени рекомендуем Вам полностью прочитать задание перед началом выполнения каких-либо работ.

Результатом выполнения задания является работоспособная сеть «из конца в конец». Самое главное, чтобы и сеть и все устройства работали. Менее важно, чтобы они работали в точном соответствии со всеми пунктами задания. Однако, как уже говорилось, за невыполнение пунктов задания команда будет терять баллы.

### **Рекомендации:**

1. Участнику рекомендуется внимательно прочитать задание и распределять время и силы.
2. Для наименьшей потери времени начать стоит с тех задач, в которых вы более уверены. Если у участника возникает затруднение, то имеет смысл выполнять следующие этапы задания наперёд - всё равно это время будет потрачено с пользой и сэкономит ресурсы в дальнейшем.
3. Для получения справочной информации в зале присутствует «интернет-кафе». Сеанс работы - 10 минут в порядке живой очереди.

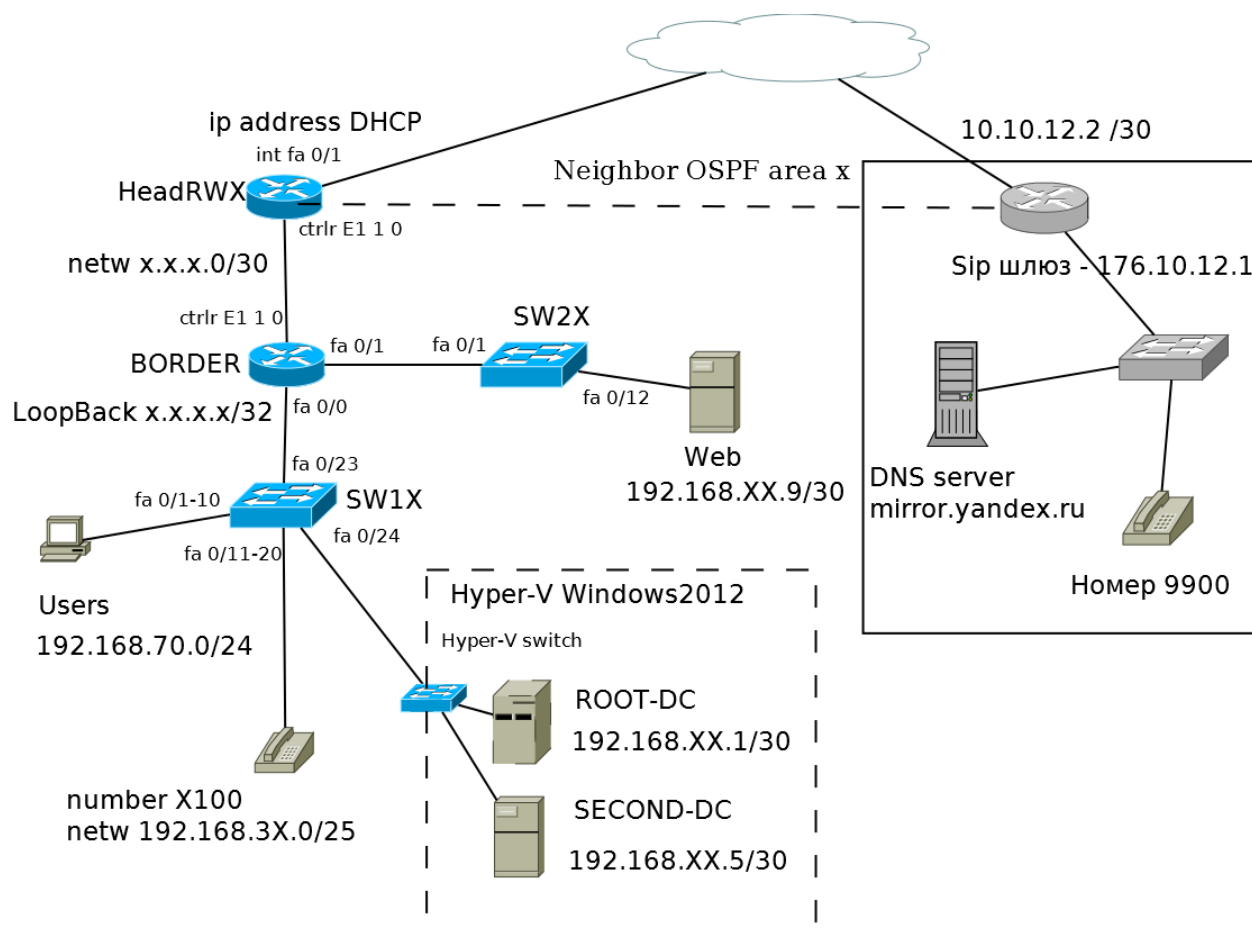
Убедитесь, что:

1. У вас нет личных вещей, запрещённых правилами - телефоны, справочная литература, устройства записи и т. д.

## Общее описание:

Ваш сегмент сетевой топологии невелик, однако, впереди много работы.

## Топология сети



Ваша задача – реализовать полностью работоспособную сеть, на основе которой будут функционировать пользовательские сервисы.

## Заметки

- Рекомендуем начать с настройки коммутатора SW1X.
- Административный VLAN настраивается на обоих коммутаторах в верхнем (по номеру) доступном порту Fast Ethernet, после коммутации основной схемы.
- В приложении есть таблица всех существующих VLAN и номера сетей которые работают в данных VLAN

## Конфигурация роутера SW1X

На данном коммутаторе необходимо выделить VLAN в соответствие с прилагаемой схемой. Для серверов AD выделите VLAN 1X и VLAN 2X соответственно, где X - номер

рабочего места. Для телефонии – VLAN3X. Для группы Users выделите VLAN 70. Административный VLAN для всех устройств - 100.

На устройстве обеспечить доступ по Telnet в административном Vlan.

Далее:

- Перевести все порты в режим согласования **desirable**
- Все порты перевести полный дуплекс
- Обеспечить доступ к устройству через telnet по административному VLANc паролем WSRX, где X - номер рабочего места
- Ограничить скорость для группы Users до 10 Mb/ps, по каждому порту

### Конфигурация роутера SW2X

WEB сервер должен находиться в VLAN4X. Административный VLAN для всех устройств - 100. На устройстве обеспечить доступ по Telnet в административном Vlan.

Далее:

- Перевести все порты в режим согласования **desirable**
- Все порты перевести полный дуплекс
- Обеспечить доступ к устройству через telnet по административному VLANc паролем WSRX, где X - номер рабочего места

### Конфигурация роутера BORDER

1. На основании схемы, подключить внутреннюю сеть, выделить необходимые саб-интерфейсы. На интерфейсах Fast Ethernet роутера назначить старший IP адрес в диапазоне. Интерфейсу Serial - назначить старший адрес сети.
2. Настроить выдачу адресов для клиентов по протоколу DHCP, исключить из выдачи адреса, назначенные саб-интерфейсам роутера. В качестве DNS-сервера указать адрес 172.10.0.2
3. Разрешить весь входящий трафик в сторону Web-сервера только для протоколов HTTP, HTTPS, POP3 (ssl), SMTP (ssl), XMPP (ssl). Остальной трафик запретить.
4. Разрешить трафик до Web-сервера по протоколу SSH только из административной сети.
5. Настроить Dial-Peer на номер 9900 через шлюз 176.10.12.1. Данная сеть должна быть получена анонсом по протоколу OSPF, в который мы анонсируем свою сеть с VOIP- телефонией.
6. Настроить Intervlanrouting для работоспособности группы Users и сервера AD
7. Разрешить входящий трафик только инициализированный изнутри и трафик для VOIP телефонии
8. Внешняя сеть на роутере BORDER оформлена на интерфейсе ctrl e1. Перевести в режим FrameRelay, выделить соответствующий Serial порт. Назначить старший адрес сети.
9. Указать маршрут по умолчанию на HeadRWX

### Конфигурация роутера HeadRWX

1. Внешний интерфейс настроить на получение адреса по DHCP. Serial интерфейсу на ctrl E1, дать младший адрес сети.
2. Настроить NAT для маскардинга сети Web-сервера

3. Настроить проброс необходимых портов для функционирования Web-сервера, Mail-сервера, ejabberd.
4. Настроить статический маршрут до LoopBack- интерфейса BORDER
5. Настроить NAT для группы Users
6. С компьютера группы Users проверить доступность внешнего Web-сервера по адресу WSR-Vologda.com
7. Проверить доступность внутреннего Web-сервера по адресу WSR-X.com

### **Конфигурация протокола OSPF**

1. Запустить процесс OSPF
2. Указать соседа по адресу 10.10.12.2 номер зоны - номер вашего рабочего места
3. Анонсировать адрес LoopBack BORDER как адрес внутренней сети
4. Получить адрес внутренней сети соседа 176.10.12.1
5. Запретить анонс остальных сетей и отключить авто суммирование маршрутов
6. Проверить доступность сети соседа (подсказка протокол использует хост и порт. ICMP закрыт по умолчанию)

### **Настройка телефонии**

1. Настроить маршрутизатор BORDER для работы VOIP по протоколу SCCP
2. В качестве адреса сервера регистрации указать LoopBack интерфейс
3. Проверить наличие звонков внутри своей телефонной сети
4. Настроить Dial-Peer во внешнюю сеть соседа по OSPF
5. Проверить наличие звонка на номер 9900

### **Заметки:**

- Используйте конфигурацию по умолчанию, если не указаны какие-либо детали.
- Топология сети участников должна в точности совпадать топологии сети в задании.
- Применять перераспределение маршрутов, статическую маршрутизацию, создавать дополнительные интерфейсы/Саб интерфейсы, если это явно не оговорено, запрещено. В случае возникновения сомнений, обратитесь к эксперту.
- Перед оценкой, все ваше оборудование будет перезапущено (перезагружено).

## Второй день

Сегодня вам предстоит настроить сервер, для управления пользователями и сервисами вашего предприятия. Вам дан сервер с Windows 2012 R2, используйте его как гипервизор. На данном гипервизоре необходимо настроить vlan, подключаться к коммутатору данный компьютер должен по 1 проводу. Обычно два контроллера домена строятся на двух разных аппаратных платформах, чтоб в случае выхода из строя обеспечить отказоустойчивость. Но в данный момент не будем это учитывать.

Так как в вашем предприятии ожидается большое количество рабочих машин вам необходимо обеспечить автоматическую установку через сеть, а так же обеспечить сохранение документов пользователей. Для связи внутри фирмы, с сотрудниками находящимися на выезде используем сервер ejabberd работающий по протоколу XMPP, не забудьте защитить внешнее подключение сервера шифрованием.

Для упрощения в обозначении примем, что X это номер вашей фирмы. В качестве сети будет использоваться та инфраструктура, которую вы настраивали в первый день. Так же вам будет выдано программное обеспечение:

2012\_64Bit\_Russian\_Core\_MLF\_X18-27640.iso – Windows2012 R2

ubuntu-15.10-server-amd64.iso – Ubuntu server

Windows 7 SP1 x86-x64 RU\_AIO.iso – Windows 7 для WDS

**По пунктам документируем все свои действия в журнале.**

**Пароль для Администратора во всех системах Windows2012 WsrVol2016.**

**Логин на WEB сервере wsr, а пароль WsrVol2016.**

Подготовка

1. Согласно приложению настроим сетевые интерфейсы и имена серверов. Введем оба сервера в домен WSR-X.com.
2. На оба сервера установите DNS сервера и настройте их таким образом, чтоб они отсылали друг другу информацию о прямых и обратных зонах просмотра. Так же они должны пересылать все неизвестные DNS имена на DNS сервер 8.8.8.8
3. **Все три сервера должны быть доступны по доменным именам. ROOT-DC.WSR-X.com, SECOND-DC.WSR-X.com, WEB.WSR-X.com.**
4. WSR-X.com должен быть доступен из локальной сети по внутреннему адресу и недоступен по внешнему (по умолчанию за это должны отвечать настройки роутера CMEX).

ROOT-DC (WIN2012)

1. Согласно приложению создайте пользователей домена и папки для каждого пользователя. После первого входа в систему, пользователи должны сменить пароль.

2. Настройте дисковые квоты согласно приложению.
3. Настройте резервное копирование данных через стандартную утилиту. Для этого самостоятельно создайте пользователя Backup и задокументируйте его логин и пароль. Резервные копии должны отправляться на второй сервер раз в день.
4. Исключите из резервного копирования такие файлы как mp3, wav, iso, avi, mpg.
5. Настроить сайты (разделение AD) и службы так чтоб оба сервера находились в разных сайтах, и репликация между ними производилась каждые 20 минут.
6. Проверьте настройки DHCP сервера, так чтоб клиенты видели оба контроллера домена.
7. [Введите в домен WSR-X.com виртуальную машину установленную на ноутбуке.](#)

## SECOND-DC (WIN2012)

1. На сервере SECOND-DC поднять роль WDS и настроить на ней раздачу образа windows 7. WDS настроить так чтоб принимались запросы от любого компьютера, даже не входящего в АД.
2. Добавить к настройкам DHCP (на роутере dhcp option 43, 47) соответствующие настройки. Проверить работоспособность, используя еще одну виртуальную машину. Устанавливать операционную систему не нужно.
3. Выделите на этом сервере каталог для резервного копирования. Настройте сетевой доступ, но так чтоб только Администратор и специальный пользователь мог видеть и изменять файлы.
4. Настройте обратные зоны DNS. На ROOT-DC данные зоны должны перейти автоматически.
5. Настройте Network Time Protocol сервер на данной машине. Время не должно синхронизироваться с серверами интернета. И обеспечьте автоматическое распространение данных настроек через сеть.

## WEB (Ubuntu)

1. Сервер WEB должен входить в DMZ зону. В первый день вы должны были обеспечить доступ в DMZ, для работы всех указанных сервисов установленных на данном сервере. Трафик соответствующих сервисов должен входить в DMZ как из локальной сети фирмы так и из интернета. Доступ в интернет из локальной сети обеспечивается по средствам NAT.
2. [Сгенерируйте сертификат с параметрами указанными в приложении используя OpenSSL на WEB сервере. Установите данный сертификат на ноутбук. Скопируйте все файлы сертификата и ключ на рабочий стол ноутбука.](#)
3. Установите web сервер Nginx. Поместите страницуIndex.html, представленную в приложении по адресу [http\(s\)://web.WSR-X.com](http(s)://web.WSR-X.com)
4. [Используйте сгенерированный сертификат для web сервера.](#)
5. Настройте автоматическое перенаправление стандартного порта webсервера на безопасный, с использованием сертификата.
6. Настройте ejabberd сервер. Он должен работать как из корпоративной сети, так и из интернета.
7. [Используйте сгенерированный сертификат для ejabberd сервера.](#)
8. Сделайте так, что - бы пользователи могли самостоятельно регистрироваться на ejabberd сервере и установите по умолчанию русский язык.
9. [Настройте почтовый сервер используя postfix и devcot.](#) Что бы можно было принимать и получать с него почту как из интернета, так и из корпоративной сети.

10. Используйте сгенерированный сертификат для почтового сервера.
11. Для почтового сервера создайте пользователей используя список пользователей Windows.
12. В базе данных должен быть создан индивидуальный пользователь для почтового сервера. Данный пользователь должен иметь полные права только на свою базу с любого адреса локальной сети. Логин и пароль должны быть записаны в журнал. Для пользователя root, у которого полный доступ ко всем базам данных, установите пароль WSR-X. Пользователь root должен подключаться только по локальному адресу своего компьютера.



## Приложение

### Таблица VLAN

VLAN	Сеть	Примечание
1X	192.168.XX.0/30	ROOT-DC
2X	192.168.XX.4/30	SECOND-DC
3X	192.168.3X.0/25	VOIP
4X	192.168.XX.8/30	WEB
70	192.168.70.0/24	Users
100	192.168.100.0/30	Admins

### Сервера

Название	Сетевой адрес	Установленные роли и службы	Примечание
ROOT-DC (WIN2012)	192.168.XX.1/30 VLAN 1X	Hyper-V, AD, DNS, Backup.	На виртуальной машине
SSECOND-DC (WIN2012)	192.168.XX.5/30 VLAN 2X	AD, DNS, WDS.	На виртуальной машине
WEB(UBUNTU)	192.168.XX.9/30 VLAN 4X	WEB-server, Почта, ejabberd- сервер.	

### Пользователи домена WSR-X.com (пользователи почтового сервера)

Не забудьте создать подразделение WSR-X

Группа пользователей	Имя пользователя	Пароль	
Администрация	Director	HcNNB976xB	
Администрация	Buxgalter	FkqmMrC6tJ	
Пользователи	User1	JfY3dzxwNV	
Пользователи	User2	8OtWlx9rE3	
Пользователи	User3	S74Tat3yGi	
Пользователи	User4	JNoYqHuyKH	

## Дисковые квоты

Объем дискового пространства между пользователями определенной группы распределяется поровну. Все расчеты документируйте.

Общий объем папки не должен превышать 150 Gb		
30 % администрация	40 % пользователи	30 % общая папка

## Страничка для WEBсервера

Страница Index.html:

```
<html>
<br><br><br><br>
<body bgcolor="white">
<h1><center><font color="black">
<imgsrc="logo.jpg" border=0><br>
Приветствуем участников соревнований. <br>
Добро пожаловать на наш веб сервер <br>
Мы группа номер X. <br>
</font>
</h1></center><br>
<br><br><br><br>
</html>
```

Параметры сертификата

Ключ для сертификата	2048 bit
название компании	WSR-X
имя сайта	WSR-X.com
email	admin@WSR-X.com
пароль	WSRnXn2016

не указанные параметры на ваше усмотрение