Второй всероссийский конкурс профессионального мастерства
«Национальный чемпионат WorldSkills Russia 2014»

Компетенция: IT Сетевое и системное администрирование

Конкурсное задание для ознакомления и подготовки участников

Для чего нужен этот документ?

В данном документе содержится задание, с которым предлагается познакомить участников, и на основании которого стоит осуществлять подготовку к национальному чемпионату.
Это задание фактически является заданием с прошедшего в 2013 году чемпионата в г. Тольятти. Задание чемпионата 2014 года в г.Казань будет достаточно похожим в части требуемых навыков у участников. Нужно понимать, что какие-то конкретные задачи из данного будут использованы на чемпионате, а какие-то добавятся, в соответствии с техническим описанием компетенции.
При подготовке участников нужно уделить внимание всем пунктам этого задания, так как участникам придется решать такие же задачи, или очень похожие.

Ключевые отличия задания чемпионата 2014 в Казани.

1. Одной из задач Всероссийского чемпионата 2014 года – подготовка к международному соревнованию EuroSkills, которое состоится осенью 2014 года. На EuroSkills по данной компетенции традиционно применяется практика состязания в командном зачете. Поэтому Национальный чемпионат России в этом году также будет проходить в командном зачете. Участники будут работать в командах по 3 человека. Участники команд должны демонстрировать слаженную совместную работу.
   Поэтому конкурсное задание будет переформировано под командный зачет. Вместо трех отдельных дней (как описано ниже), задание будет состоять из одного комплексного трехдневного проекта, который предстоит выполнить команде.
2. В национальном чемпионате 2014 планируется, в соответствии, с международным опытом, включить в задание работу с межсетевыми экранами Cisco ASA 5505 / 5510. Участникам будет предложено продемонстрировать навыки работы с подобными устройствами и с их помощью обеспечить функционирование защищенных VPN соединений.
3. Задание национального чемпионата будет комплексным. Это означает, что одни технологии будут тесно переплетаться с другими. Как результат, например, ошибки, допущенные в третьем дне могут повлиять на работу уже настроенных конфигураций первого дня и наоборот, а неполадки в одной части сети могут повлиять на работу всей сети. Во время оценки будет проверяться комплексная работа всей инфраструктуры. Поэтому очень важно эффективное взаимодействие между участниками команды, постоянный контроль выполняемых действий, а также хорошее понимание у всех участников во всех сферах выполняемой командой работы, а не только в своей области (напр. один участник умеет настраивать маршрутизацию на Cisco, но не может работать с Lunix сервером).

Секция 1.

1. Уважаемый участник, поздравляем вас с назначением на должность главного специалиста по ИТ-инфраструктуре в компании WSR-Russia. Надеемся, что наше сотрудничество будет продуктивным и взаимовыгодным. Прежде всего, мы хотели бы чтобы вы выполнили одно важное задание для нас. Дело в том, что совсем недавно нами был открыт новый филиал в г.Тольятти, и мы бы хотели направить вас туда, для создания необходимой ИТ-инфраструктуры в новом офисе компании. В Тольятти, офисы компании располагается в двух зданиях. Вы будете обеспечены всем необходимым оборудованием и материалами для выполнения этой нелегкой миссии. Прежде всего, в офисе необходимо построить СКС, выполнить монтаж оборудования в коммутационный шкаф.
    a. Установить оборудование в коммутационный шкаф в следующем порядке:
        - WSR_R1;
        - WSR_R2;
        - Патч-панель;
        - Кабель-органайзер;
        - WSR_SW1;
    b. На гипсокартонном блоке установить 3 информационные розетки RJ-45.
    c. Расшить кабель (витую пару) в информационные розетки RJ-45 и патч-панель, в порты 1, 2, и 3 соответственно. Провода должны быть уложены в гофро-трубу. Использовать для подключения к консольному порту оборудования.
    d. Для подключения рабочих станций проложить отдельной гофро-трубе необходимое количество кабелей.
    e. Закрепить клипсами гофро-трубу на гипсокартонном блоке.
    f. Оконечить провода коннекторами RJ-45 для подключения оборудования в соответствии со стандартом TIA/EIA 568. Необходимо использовать правильные типы кабеля для соединения (прямой или перекрестный).
    g. Произвести коммутацию сетевого оборудования и рабочих станций в соответствии с заданной топологией.
2. Произвести настройку всего сетевого оборудования.
    a. Задать пароль cisco на вход в привилегированный режим всего сетевого оборудования.
    b. Задать имя сетевого оборудования в соответствии с топологией.
    c. Для удобства управления сетевым оборудованием, настроить возможность удаленного подключения:
        - Создать пользователя WSR с паролем 2013 и наивысшим уровнем привилегий;
        - Установить локальную аутентификацию по умолчанию;
        - Пользователь WSR должен автоматически попадать в привилегированный режим.
    d. На коммутаторе:

- Отключить динамическое согласование транков на всех портах коммутатора;
- Настроить VTP домен WSR в режиме, не распространяющем информацию из базы ВЛВС, с паролем wsr_2013;
- Создать виртуальные локальные сети (ВЛВС) согласно приложению 1.2;
- Настроить виртуальный интерфейс 3-го уровня для удаленного управления коммутатором в управляющей подсети.
- Настроить магистральные (транковые) порты согласно топологии; На транковых портах разрешить только ВЛВС необходимые для данной топологии.
- Иногда, при подключении в сеть, компьютеры не могут получить долгое время (по заявлениям пользователей) получить IP-адрес по протоколу DHCP. Предоставьте решение данной проблемы на портах f0/1 и f0/2.

e Маршрутизаторы:

- Задать доменное имя устройства wsr.ru;
- Настроить интерфейс FastEthernet0/0 каждого маршрутизатора используя сабинтерфейсы для каждой ВЛВС. Настроить IPv4 адреса на интерфейсах маршрутизатора в со схемой топологии;
- Настроить логические интерфейсы;
- Настройка виртуальных терминальных линий:
  - Установить синхронный вывод событий в терминал;
  - Установить тайм-аут exec-процесса 3 минут.*
- Настроить протокол SSH:
  - Версия протокола — 2;
  - Количество попыток аутентификации — 5;
  - Укажите минимальную длину ключа, необходимую для работы протокола SSHv2.
- Установить блокировку входа на 2 минуты в случае 3 неудачных попыток в течении 20 секунд. Исключением для блокировки должны быть адреса Management ВЛВС.
- Установить задержку входа 5 секунд.
- Создать пользователя root с паролем toor. Данная учетная запись должна автоматически удаляться после первого удачного входа в систему.

3 Как вы знаете, наша политика безопасности требует создания выделенной сети управления всем сетевым оборудованием. Вам необходимо создать и обеспечить безопасность сети управления. В сети управления запрещен любой пользовательский трафик. На интерфейсах маршрутизаторов, подключенных к сети управления:

a Разрешен исходящий трафик только до адресов из сети управления, на порты **пяти** основных протоколов удаленного управления сетевым оборудованием.

b Разрешен входящий трафик только от адресов из сети управления на адрес маршрутизатора из этой же сети, на порты **пяти** основных протоколов удаленного управления сетевым оборудованием.

4. Для обеспечения связи между двумя офисами, мы приобрели две выделенные линии связи, и постарались максимально обезопасить их от несанкционированного доступа. Для обеспечения безопасности мы попросили провайдеров ограничить возможные IP адреса отправителей только IP адресами соответствующих интерфейсов маршрутизаторов (см. схему) Вам необходимо настроить динамический протокол маршрутизации RIPv2 между двумя маршрутизаторами. Для обмена маршрутной информации необходимо использовать только сегменты 172.16.1.0 и 172.16.2.0. Пакеты RIP не должны распространяться через интерфейсы, подключенные к другим сетям.

   a. Для проверки работоспособности выделенной линии предполагается в будущем использовать технологию IP SLA. Для работы IP SLA Вам необходимо обеспечить возможность успешной отправки ICMP запросов и получения ICMP ответов между каждой парой интерфейсов маршрутизаторов подключенных к одному сегменту (без учета ВЛВС управления).

5. В каждом офисе запланирована своя IPv6 подсеть, однако провайдер не поддерживает IPv6. На интерфейсах маршрутизаторов, подключенных к сегментам 172.16.1.0 и 172.16.2.0 не должно быть IPv6 адресов.

6. Для обмена маршрутной информацией о IPv6 сетях, необходимо настроить протокол динамической маршрутизации OSPFv3. Правильное выполнение задания позволит рабочим станциям обмениваться IPv6 трафиком. Вам необходимо обеспечить отказоустойчивость соединений по протоколу IPv6 между двумя офисами за счет протокола маршрутизации IPv4.

   a. Интерфейс маршрутизатора WSR_R1 подключенный к WSR_HOST1 поместить в OSPFv3 зону 1.

   b. Интерфейс маршрутизатора WSR_R2 подключенный к WSR_HOST2 поместить в OSPFv3 зону 2.

   c. Виртуальный интерфейс между маршрутизаторами WSR_R1 и WSR_R2 поместить в OSPFv3 backbone.

7. В офисе №1 будет находится рабочая станция нашего единственного сотрудника. В качестве ОС, он предпочитает Windows 7.
   - В ходе установки вам необходимо создать два раздела на жестком диске
     - Раздел для операционной системы (30% дискового пространства);
     - Раздел для пользовательских данных (70% дискового пространства).
   - Создайте учетную запись wsr_user и добавьте его в группу локальных администраторов*;
   - Установите дополнительные компоненты операционной системы: клиент службы Telnet;
   - Сконфигурируйте на сетевом интерфейсе ПК IPv6 адрес согласно схеме адресации.

8. Во втором офисе будет находится наш сервер на FreeBSD. При установке FreeBSD:
   a. Разметить жесткий диск следующим образом:
      - / - 10Гб;
      - /var - 10Гб;
      - /usr - 20Гб;

- swap - 4Гб.

b. На сетевом интерфейсе настройте IPv6 адрес согласно разработанной схеме адресации.

c. Для соблюдения корпоративной политики безопасности отключите возможность доступа по Telnet и настройте возможность доступа по SSH только через порт 65022;

d. Также, вам необходимо настроить парольную политику:
   - Пароль должен состоять из символов принадлежащих, как минимум 3-м классам (например, верхний и нижний регистр, цифры);
   - Длина пароля не должна быть меньше 8 символов и превышать 15 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 root используя su;
   - При создании пользователя, в параметрах по умолчанию, должен генерироваться случайный пароль, отвечающий критериям данной политики;
   - После создания пользователя, при его первом входе в систему (как локально, так и по SSH), система должна запрашивать смену пароля. Новый пароль также должен отвечать критериям данной политики.

e. Настроить IPv6 DNS-сервер (с помощью BIND) для зоны wsr.local:
   - Создать две зоны: прямую и обратную, где зарегистрировать все устройства (в том числе сетевые);
   - Используя утилиты ping, nslookup проверить работоспособность и доступность сервера.

f. Настройка IPF:
   - Разрешить доступ для DNS-запросов;
   - Разрешить доступ по SSH через порт 65022;
   - Разрешить ICMP ECHO;
   - Запретить все остальные запросы;
   - IPF должен запускаться автоматически при старте системы.

9. Проверка работоспособности сетевой инфраструктуры:

   a. В таблице маршрутизаторов должны содержаться только сети, подключенный напрямую и информация из динамических протоколов маршрутизации;

   b. Все устройства могут посылать друг другу ICMP ECHO запросы по имени и получать ICMP ECHO ответы.

10. Обновить операционную систему маршрутизатора WSR_R1, скачав ее с TFTP-сервера.

Приложения к секции 1.

Приложение 1.1 Схема IPv6 адресации

Сегмент	**Сеть**	**Узел**	**Адрес**
WSR_R1 <-> WSR_HOST_1	FEC0:1:C1C0::0/124	WSR_R1	FEC0:1:C1C0::1/124
WSR_R1 <-> WSR_HOST_1	FEC0:1:C1C0::0/124	WSR_HOST_1	FEC0:1:C1C0::C/124
WSR_R2 <-> WSR_HOST_2	FEC0:2:C1C0::0/124	WSR_R2	FEC0:2:C1C0::1/124
WSR_R2 <-> WSR_HOST_2	FEC0:2:C1C0::0/124	WSR_HOST_2	FEC0:2:C1C0::C/124
WSR_R1<-> WSR_R2	FEC0:12:C1C0::0/124	WSR_R1	FEC0:12:C1C0::A/124
WSR_R1<-> WSR_R2	FEC0:12:C1C0::0/124	WSR_R2	FEC0:12:C1C0::B/124

Приложение 1.2 Создание ВЛВС на коммутаторе 3го уровня

VLAN ID	**Имя**
100	ISP2
200	WSR300
300	WSR200
252	Management

Приложение 1.3 Адресация управляющей подсети

Устройство	**Адрес**
WSR_R1	172.16.252.1 /24
WSR_R2	172.16.252.2 /24
WSR_SW1	172.16.252.3 /24

Секция 2

ПИСЬМО

Главному администратору
ООО “Лучшие технологии”
от Генерального директора

Дорогой друг, перед вами стоит ответственная задача создания информационной инфраструктуры в новом центральном офисе нашей компании. Вам будут доступны лучшее оборудование и ПО ведущих мировых производителей. Надеюсь, вы оправдаете мое доверие, и рационально распорядитесь доступными вам ресурсами. Прошу обратить внимание, на необходимость обеспечения высокого уровня информационной безопасности в создаваемой вами информационной инфраструктуре. Для того, чтобы вы могли как можно скорее приступить к выполнению своих обязанностей, я составил для вас небольшой план действий:

1. Поскольку, сетевая инфраструктура является фундаментом всей информационной инфраструктуры, важно правильно заложить этот фундамент. С целью обеспечения должного уровня информационной безопасности в сети, на всем сетевом оборудовании:
    a. Настроить удаленное системное журналирование на сервере Fedora Linux:
        - Настроить журналирование удачных и неудачных попыток входа;
        - Включить в журнал все сообщения об ошибках.
    b. Обеспечить защиту от вывода из строя сетевого оборудования путем удаления файла операционной системы Cisco IOS с последующей перезагрузкой.
2. На всех коммутаторах создать ВЛВС согласно приложению 2.1.2;
3. На всех портах коммутаторах рабочей группы, за исключением портов Switch-to-Switch и Switch-to-Router
    a. Настроить Port security:
        - Фреймы, вызвавшие нарушение безопасности должны быть отброшены, уведомление о нарушении не должны генерироваться, порт должен оставаться активным;
        - Использовать автоматическое добавление безопасных MAC-адресов в конфигурационный файл.
4. ВЛВС 300 будет использоваться для передачи данных, критичных для нашего бизнеса. Очень важно правильно настроить коммутаторы, чтобы свести к минимуму задержку при изменении L2 топологии:
        - Используйте на коммутаторах протокол STP, обеспечивающий с одной стороны расчет покрывающего дерева для каждой ВЛВС в отдельности, с другой стороны позволяющий коммутаторам непосредственно обмениваться BPDU друг с другом;
        - Коммутатор WSR_SW3 должен являться корнем связующего дерева в ВЛВС 300;

- В случае выхода из строя коммутатора WSR_SW3, коммутатор WSR_SW2 должен стать новым корнем связующего дерева в ВЛВС 300;
- В случае выхода из строя коммутатора WSR_SW2, коммутатор WSR_SW1 должен стать новым корнем связующего дерева в ВЛВС 300;
- С точки зрения отказоустойчивости, все коммутаторы объединены двойным кольцом. Пожалуйста, в ВЛВС 300 используйте для передачи данных внутреннее кольцо (т.е. для коммутаторов WSR_SW1 и WSR_SW3 порт 0/11 должен быть заблокирован, а порт 0/12 должен передавать данные и т.д.). При выполнении задания запрещено менять параметр стоимости пути протокола связующего дерева.

5. К сожалению, коммутаторы третьего уровня находятся еще в пути, надеюсь что вы сможете организовать маршрутизацию между ВЛВС с использованием всего лишь одного интерфейса маршрутизатора. В качестве IP адреса для соответствующих интерфейсов использовать последний доступный IP адрес из подсети ВЛВС.
6. В нашей организации всего один физический сервер, а поскольку для решения бизнес задач нам потребуются сразу несколько серверов с различными ОС, такие как Windows Server и Fedora Linux, нам понадобятся некоторые возможности виртуализации. Установите гипервизор VMware ESXi 5.0 Update 2 на наш физический сервер:
   a. Назначьте пароль для root – P@ssw0rd;
   b. Установите статический IP адрес на управляющем интерфейсе;
   c. Мы хотим быть уверенными в том что наш гипервизор не подведет нас в самый ответственный момент поэтому задайте параметры резервирования ресурсов для сервисной консоли гипервизора:
      - Процесорного времени : 600 Mhz;
      - Оперативной памяти: 768 Mb.
   d. Создайте Port Group на виртуальном коммутаторе согласно приложению 2.2;
   e. Наш главный администратор предпочитает управлять гипервизором с помощью командной строки при помощи клиента putty, поэтому настройте доступ по протоколу ssh;
   f. Безопасность должна быть безопасной! Сконфигурируйте брандмауэр гипервизора в соответствии с Приложением 2.3;
   g. Для нашей организации время очень ценно и мы не можем позволить себе потерять ни минуты. Сконфигурируйте клиент NTP сервисной консоли.
7. Создайте виртуальную машину и установите ОС Fedora Linux
8. Создайте виртуальную машину (ВМ) DC01. На ВМ установите ОС Windows Server 2008 R2 в соответствии с Приложением 2.6.
   a. Выполните сетевую конфигурацию, задайте имя сервера DC01;
   b. Поскольку наша компания динамично развивается, предполагается появление в скором времени большого числа пользователей и парка машин, соответственно потребуется централизованное управление и контроль над ними, поэтому было решено воспользоваться возможностями Активного Каталога MS AD. Разверните

домен Active Directory (wsr.ru) на сервере dc01, в процессе установите и настройте роль DNS сервера;

c Вам доверено заняться двумя нашими новыми отделами - Отделом ИТ и Отделом Продаж. Создайте OU “Отдел ИТ” и “Отдел продаж”;

d Создайте группы безопасности “IT” и “Sales” соответственно;

e Создайте уч. записи пользователей в домене wsr.ru в соотв. с приложением 2.7.

9 Установите и настройте работу DHCP-сервера; Выдать IP адреса рабочим станциям сотрудников из ВЛВС 300 и из сети 10.10.0.0/18.

10 Выполните настройку ноутбука 1, назовите машину WS-IT01, сетевые параметры - автоматически. Введите компьютер в домен wsr.ru.

11 Выполните настройку ноутбука 2, назовите машину WS-Sales01, сетевые параметры - автоматически. Введите компьютер в домен wsr.ru.

12 Для надежного и удобного хранения всех данных пользователей организации было решено доверить вам развертывание файлового сервера.

a Создайте виртуальный диск в соответствии с Приложением 2.6 и подключите к ВМ DC01;

b Отформатируйте новый диск в NTFS том и назначьте букву логического диска - E:

c Установите роль файлового сервера, создайте сетевые папки в соответствии с Приложением 2.8;

d Поскольку вычислительные ресурсы нашей организации ограничены, вам было поручено взять под контроль использование дискового пространства файлового сервера. Настроите квоты и фильтрацию для сетевых папок в соответствии с Приложением 2.9.

13 Для работы с тяжелыми приложениями в нашей компании будет использоваться терминальный режим доступа. Для этого создайте ВМ - Term01 в соответствии с Приложением 2.6.

a Настройте сетевые параметры ОС;

b Добавьте сервер в домен wsr.ru.

14 На сервере Term01.wsr.ru Установите и настройте роль Терминального сервера

- 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 веб для всех сотрудников отдела ИТ;
- Опубликуйте программу “Calc” ” на веб портале RemoteApp для пользователя User1;
- Создайте MSI пакеты RemoteApp для приложений Wordpad и Notepad, они вам еще пригодятся.

15 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 в соответствии с приложением 2.10 (WSR_Policy);
- В нашей организации постоянно думают о том как повысить удобство пользования внутренними сервисами для сотрудников компании, а также 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 (Deploy_RA_IT) и notepad для пользователей Отдела Продаж (Deploy_RA_Sales));
- 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 ИТ в локальную группу администраторов для всех компьютеров (ноутбуков) домена (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, Net_Share_IT);
- Для повышения стабильности и безопасности ИС на терминальном сервере term01.wsr.ru запретите применение любых пользовательских политик (Term_Loopback);
- У нас очень дружный и сплоченный коллектив поэтому все сотрудники должны быть в курсе последний новостей нашей компании. При помощи групповых политик домена, настройте стартовую страницу в браузере IE, для всех сотрудников, на сайт компании wsr.ru (IE_StartPage);
- Наша служба поддержки не очень любит много передвигаться по зданию, и все больше решает проблемы пользователей по телефону. При помощи групповых политик домена, включите удаленный рабочий стол на всех компьютерах пользователей домена (RDP_ON);
- Мобильность пользователей и сохранность их данных один из приоритетов нашей организации, поэтому, при помощи групповых политик домена, включите перенаправление папок для пользователей user1 и user2 на файловый сервер (Рабочий стол, Мои документы) (Folder_Redirect);
- 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 кроме Отдела_ИТ (Sales_Desk_Theme).

16 К сожалению в нашей организации пока что не выделили средства на надежную систему бесперебойного электропитания, а ночью часто случаются перебои с электричеством, следует позаботиться о том чтобы с утра все наши сервисы, в том числе виртуальные машины работали. На гипервизоре настройте автозапуск ВМ в нужном порядке;

17 Сохранность информационных сервисов и данных пользователей очень критично для нашего бизнеса поэтому мы просто обязаны подстраховаться и иметь систему резервного копирования. На сервере DC01.wsr.ru настройте расписание резервного копирования на сервер Fedora Linux по протоколу SMB и настроите расписание резервного копирования:

- в резервную копию должны включатся файлы каталогов файлового сервера, а также состояние системы включая службы каталогов. Период создания резервных копий - один раз в час*;
- проверьте работу резервного копирования на стороне клиента*;
- проверьте работу резервного копирования на стороне сервера и наличие резервных копий в каталоге Backup*.

Приложения к секции 2.

Приложение 2.1.1 Адресация управляющей подсети

Устройство	**Адрес**
WSR_R1	192.168.252.10
WSR_SW1	192.168.252.20
WSR_SW2	192.168.252.30
WSR_SW3	192.168.252.40
SRV (ESX)	192.168.252.50

Приложение 2.1.2 Таблица ВЛВС коммутаторов

№ ВЛВС	**Имя**	**Сеть**
100	SC	192.168.100.0/24
101	VM1	192.168.101.0/24
102	VM2	192.168.102.0/24
200	VMK	192.168.103.0/24
252	Management	192.168.252.0/24
300	Critical	192.168.255.0/24

Приложение 2.2

Вирт. Коммутатор	**Порт группа, Vlan.**	**Назначение/Тип**	**Uplinks**	**Политика NicTeam**
vSwitch01	Service Console Vlan 100	Менеджмент Console Тип: SC	Vmnic0 Vmnic1	Активные адаптеры: vmnic0; В режиме ожидания Vmnic1; Балансировка на основе vPortID. Оповещение свича – включено; Обнаружение обрыва на основе Link state. Шейпер отключен.
vSwitch01	VMKernel Vlan 200	NFS Vmk0	Vmnic0 Vmnic1	Активные адаптеры: vmnic1; В режиме ожидания Vmnic0 Балансировка на основе vPortID. Оповещение свича – включено; Обнаружение обрыва на основе Link state. Шейпер отключен.

vSwitch01	VM 1 Vlan 101	Группа портов для ВМ из 101 Vlan Тип: Virtual Machine	Vmnic0 Vmnic1	Активные адаптеры: vmnic0, vmnic1; Балансировка на основе vPortID. Оповещение свича – включено; Обнаружение обрыва на основе Link state. Шейпер отключен
vSwitch01	VM 2 Vlan 102	Группа портов для ВМ из 102 Vlan Тип: Virtual Machine	Vmnic0 Vmnic1	Активные адаптеры: vmnic0, vmnic1; Балансировка на основе vPortID. Оповещение свича – включено; Обнаружение обрыва на основе Link state. Шейпер отключен

Приложение 2.3

Название правила	**Порт (протокол)**
Входящие подключения	
CIM Secure Server	5989 (TCP)
SSH Server	22 (TCP)
vSphere Web Access	80, 443 (UDP, TCP)
CIM Server	5988 (TCP)
AAM	2050-2250, 8042-8045 (TCP, UDP)

Исходящие подключения	
vCenter UM	80, 9000-9100 (TCP)
SSH Client	3260 (TCP)
NTP Client	123 (UPD)
VMware CB	443, 902 (TCP)
AAM	2050-2250, 8042-8045 (TCP, UDP)
VMware vCenter Agent	902 (UDP)
NFS Client	111, 2049

Приложение 2.5

Имя для Datastore	**Размер**	**Размер блока**	**Файловая система**	**Назначение**
DS01_Local	230 GB	8 Mb	VMFS 3.46	Для ВМ
DS02_NFS	100 Gb	-	NFS	ISO образы

Приложение 2.6

ВМ	**Параметры ВМ**	**ОС**	**Сетевая конфигурация**
fedora01	1 vCPU 1 ГБ RAM 60ГБ HDD 1 vNIC PortGroup - 101	Fedora Linux	192.168.101.1 255.255.255.0 192.168.101.254 192.168.102.1
dc01	2 vCPU 2 ГБ RAM 100 ГБ HDD 500 ГБ HDD 1 vNIC PortGroup - 102	Windows Server 2008 R2 64 bit RU	192.168.102.1 255.255.255.0 192.168.102.254 192.168.102.1
term01	4 vCPU 3 ГБ RAM 100 ГБ HDD 1 vNIC	Windows Server 2008 R2 64bit RU	192.168.102.2 255.255.255.0 192.168.102.254 192.168.102.1

	PortGroup - 102		

Приложение 2.7

Уч. запись	**Организац. ед.**	**ФИО**	**Тел.**	**Член групп**
User1	Отдел продаж	Ирина Петрова	101	Domain Users Sales
User2	Отдел ИТ	Илья Лапшин	201	Domain Users IT

Приложение 2.8

Путь к папке	**Сетевой путь**
E:\Folders\Desktops	\\dc01\Desktops$
E:\Folders\Documents	\\dc01\Documents$
E:\Folders\Sales	\\dc01\Sales
E:\Folders\IT	\\dc01\IT

Приложение 2.9

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

Приложение 2.10

Атрибут	**Значение**
Вести журнал паролей	6
Максимальный срок действия пароля	42
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

Секция 3

1. Уважаемый участник, поздравляем вас с назначением на должность главного специалиста по ИТ-инфраструктуре в компании WSR-Russia. Надеемся, что наше сотрудничество будет продуктивным и взаимовыгодным. Прежде всего, мы хотели бы чтобы вы выполнили одно важное задание для нас. Дело в том, что совсем недавно нами был открыт дополнительный филиал в г.Тольятти, и мы бы хотели направить вас туда, для создания безопасной беспроводной сети стандарта WiFi, а так же для упрощения процесса печати в нашем филиале. Прежде всего, вам необходимо развернуть контроллер домена в ЦО. Добавить рабочую станцию в домен. Имя домена WSR.ru
2. Вам дана сеть 10.0.0.0 /24, необходимо разработать схему адресации в соответствии с заданной топологией. Адрес маршрутизатора — последний доступный адрес в подсети, адреса ноутбука и телефона должны быть получены по DHCP, адрес сервера — первый доступный адрес в подсети, адрес точки доступа предпоследний доступный адрес в подсети. Для адресации между маршрутизаторами использовать нечетные адреса на WSR_R1 и четные адреса на WSR_R2.
3. Настроить на сетевом оборудовании:
    a. Имена устройств (в соответствии с топологией);
    b. Шифрованный пароль cisco на в ход в привилегированный режим;
    c. Создать пользователя WSR с паролем 2013 и наивысшим уровнем привилегий;
    d. Пользователь WSR должен автоматически попадать в привилегированный режим.
4. Для обеспечения взаимосвязи ЦО и филиала настроить IPsec VPN туннель таким образом, чтобы обеспечить возможность работы любых динамических протоколов маршрутизации (RIPv2, OSPF, EIGRP):
    a. Использовать схему авторизации с общим ключом (wsr_key);
    b. Для шифрования трафика и обмена ключевой информацией использовать 3DES и SHA-1;
    c. Группа Диффи-Хелмана 16.
5. Обеспечить динамический обмен маршрутной информацией между ЦО и филиалом, используя протокол маршрутизации EIGRP с номером автономной системы 1.
    a. В любом филиале должна быть доступна сеть другого филиала;
    b. EIGRP должен в 2 раза быстрее обнаруживать отказ соседнего маршрутизатора, при работе через IPsec VPN туннель, по сравнению со стандартными параметрами;
    c. При расчете метрики, протокол EIGRP должен учитывать загруженность и надежность интерфейсов;
    d. По умолчанию, маршрутизатор не должен рассылать обновления на интерфейсы, кроме туннельного;

e При конфигурации EIGRP указывать точные адреса сетей используя обратную маску.

6 Для аутентификации мобильных пользователей, настроить роль RADIUS-сервера на контроллере домена ЦО.

7 В ЛВС филиала, настроить беспроводной маршрутизатор в режиме моста с аутентификацией WPA2 PSK, шифрование AES CCMP. DHCP-сервером для беспроводной сети должен выступать контроллер домена. Согласно корпоративной политике безопасности, клиенты беспроводной сети должны иметь доступ к корпоративной сети и интернету. Однако, доступ к корпоративным ресурсам возможен только после установки PPTP туннеля с аутентификацией через RADIUS-сервер. В случае недоступности RADIUS-сервера необходимо использовать локальную аутентификацию мобильных пользователей.

a На маршрутизаторе WSR_R1 настройте PPTP сервер;

b Клиентские машины должны получать ip-адрес из диапазона 10.0.0.X /25;

c В качестве протокола шифрования установить MPPE, длинна ключа должна подбираться автоматически;

d Установить последовательность протоколов авторизации CHAP, MS-CHAP, MS-CHAPv2;

e Для связи между мобильными пользователями и центральным офисом добавьте в протокол маршрутизации EIGRP команду redistribute connected.

8 Обеспечить телефонную связь между офисами с помощью Cisco Call Manager Express:

a На маршрутизаторе WSR_R1:

- Обеспечить возможность подключения программного телефона Cisco IP Communicator с номером 202 с ноутбука через PPTP VPN;
- Настроить маршрут звонка для номеров 2xx на маршрутизатор WSR_R2.

b На маршрутизаторе WSR_R2:

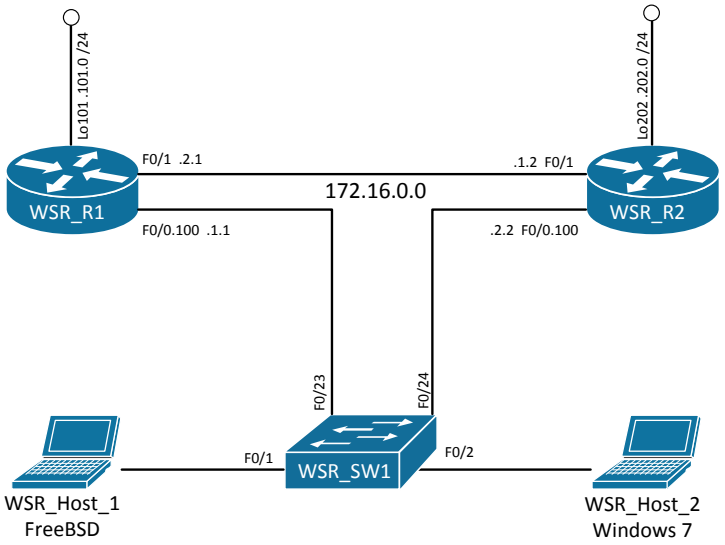
- Обеспечить возможность подключения аппаратного телефона Cisco с номером 101;
- Создайте соответствующий DHCP пул на маршрутизаторе;
- Настроить маршрут звонка для номеров 1xx на маршрутизатор WSR_R1.

9 Установить ПО Cisco IP Comminicator:

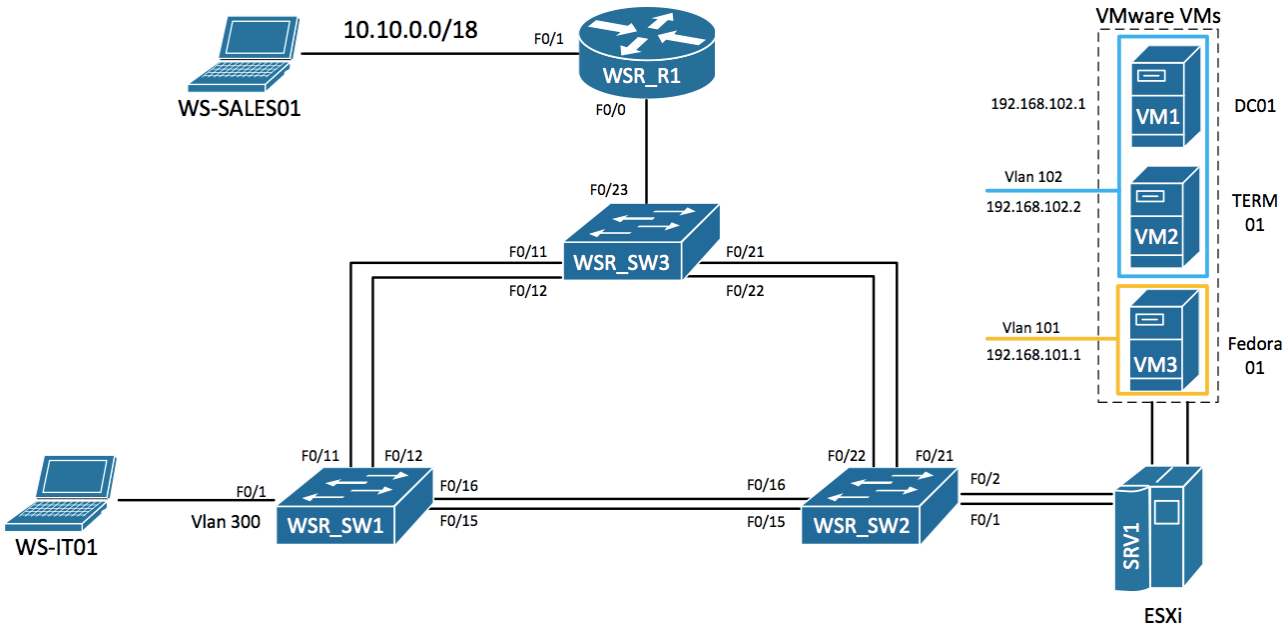
a Для установки на ноутбук использовать установку из исполняемого «exe» файла.

10 Сотрудники филиала имеют возможность позвонить в ЦО с номера 202 на 101 и наоборот.

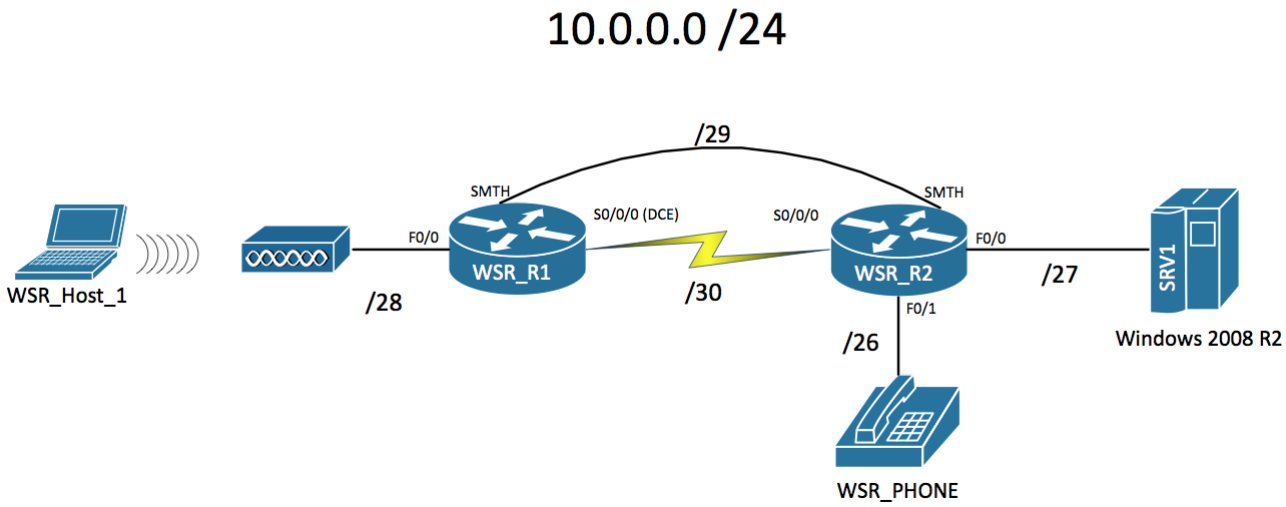
Секция 1



Секция 2



Секция 3


10.0.0.0 /24
/29
SMTH
SMTH
S0/0/0 (DCE)
S0/0/0
F0/0
F0/0
WSR_R1
WSR_R2
SRV1
WSR_Host_1
/28
/30
/27
F0/1
/26
Windows 2008 R2
WSR_PHONE