КОнкурсное задание

МЕЖРЕГИОНАЛЬНОГО чемпионата

**Сетевое и СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ**

WorldSkills Kazakhstan-2018

**ОПИСАНИЕ МОДУЛЕЙ И ЗАДАНИЙ**

Модуль № A, B, С = общая сумма оценок (100 баллов)

Участники могут ознакомиться со своей работой до начала конкурса (оборудование, материалы и т.п.)

|  |  |  |
| --- | --- | --- |
| **Описание модулей «Веб-разработка»** | **Продолжительность** | **Количество баллов** |
| **Модуль - А**  Среда Linux | 3 часа | 40 |
| **Модуль - B**  Среда WINDOWS | 4 часа | 40 |
| **Модуль - С**  Cisco Packet Tracer | 1 час | 20 |

# 1 МОДУЛЬ A

## ОПИСАНИЕ ПРОЕКТА И ЗАДАНИЙ

Вы являетесь системным инженером в только что учрежденной компании, которая занимается разработкой корпоративных сайтов.

Вашим заданием является построить новую IT-инфраструктуру для компании. Вся сеть должна быть основана на ОС Linux.

Сотрудники должны иметь возможность отправлять электронные письма, а также иметь доступ к файловым ресурсам.

Вы также должны установить удаленный доступ к VPN для фрилансеров, веб-сервер для создаваемых веб-сайтов.

Связь между клиентами и сервером должна всегда шифроваться. Дополнительная информация приведена в приложении.

# часть А1

## РАБОЧЕЕ ЗАДАНИЕ УСТАНОВКА (LNXRTR1, LNXSRV1, LNXSRV2)

Примечание: Пожалуйста, используйте конфигурацию по умолчанию, если вам не предоставили подробной информации.

Базовая ОС Debian была установлена на lnxrtr1, lnxsrv1 и lnxsrv2.

## РАБОЧЕЕ ЗАДАНИЕ СЕРВЕР LNXRTR1

* Настроить сервер с именем узла, доменом и IP-адресом, указанным в приложении
  + Установить службы:
    - Маршрутизация
      * Включить маршрутизацию
    - Межсетевой защитный экран (утилита iptables)
      * Разрешить следующие сервисы lnxsrv1 из внешней сети:
        + HTTPS
        + DNS
        + FTPS
        + SMTPS
        + IMAPS
      * Разрешить трафик из внутренней сети и сети DMZ к внешней сети.
      * Разрешить трафик от внутренней сети к DMZ
      * Разрешить следующей трафик от внешней сети по отношению к lnxrtr1
        + OpenVPN
        + Прокси-сервер (Nginx)
      * Разрешить весь трафик от внутренней сети к lnxrtr1
      * Все другие трафики должны быть запрещены.
      * Настроить источник NAT для внутреннего доступа в Интернет из внутренней сети.
      * Статические преобразования NAT
        + 192.168.10.150 <=> 32.54.87.114
      * Протокол DHCP
        + Диапазон для внутренней сети:

Диапазон: 172.17.20.100 – 172.17.20.150

Маска подсети: /24

Шлюз: 172.17.20.1

DNS: 192.168.10.150

* + - * + DNS-суффикс: site4you.kz
        + Lnxclnt2 всегда должен получать следующий IP-адрес: 172.17.20.95
        + Клиенты должны автоматически регистрировать свое имя с DNS-серверов после того, как им был назначен IP-адрес DHCP-сервером.
    - VPN (OpenVPN)
      * Настроить VPN доступ к внутренней сети. Внешние клиенты должны подключаться к 32.54.87.115
      * Убедитесь, что VPN-клиенты могут получить доступ только к серверу lnxsrv2
      * Использовать диапазон адресов с 10.2.1.1 до 10.2.1.62 для VPN-клиентов
      * Для логина создать пользователя с паролем «Skills39»
      * Использовать сертификат, подписанный lnxsrv2
    - Прокси-сервер (Nginx)
      * Настроить обратный SSL прокси-сервер для сайта www.site4you.kz, размещенного на сервере lnxsrv1
      * Для «www.site4you.kz», доступ HTTP должен быть автоматически перенаправлен на HTTPS
        + Использовать сертификат, подписанный lnxsrv2

Убедиться, что не отображается никакое предупреждение о сертификате

* + - * + Использовать аутентификацию по сертификату клиента для www.site4you.kz

Разрешить только клиентские сертификаты, подписанные lnxsrv2

## РАБОЧЕЕ ЗАДАНИЕ СЕРВЕР LNXSRV1

Примечание: Пожалуйста, используйте конфигурацию по умолчанию, если вам не предоставили подробной информации.

* Настроить сервер с именем узла, доменом и IP-адресом, указанным в диаграммах, приведенных в приложении
* Установить сервисы
  + Веб-сервер (Apache2)
    - Установить apache2, включая php5
    - Включить HTTPS
      * Использовать сертификат, подписанный lnxsrv2
        + Убедиться, что не отображается никакое предупреждение о сертификате
  + Создать веб-сайты «www.site4you.kz» и «intranet.site4you.kz»
    - Настроить /webdav для WebDAV
      * Создать и использовать каталог /data/webdav
      * Каталог «/webdav» должен быть доступен только из внутренней сети
    - Показывать на обоих сайтах имя веб-сайта (полное доменное имя) и текущую дату и время (время клиента или время сервера)
    - В качестве основной меры безопасности, убедиться, что Apache2 не подвергает опасности любой заголовок протокола и нижнюю информацию (например, версия, ОС,...).
  + DNS (привязка)
    - Убедиться, что оба сайта отображаются на 32.54.87.114 (intranet.site4you.kz) и 32.54.87.115 (www.site4you.kz) из Интернета, который уже связан с IP-адресом lnxsrv1 на lnxrtr1.
      * Запросы от внутренних сетей (Внутренние) для обоих сайтов должны поступать на внутренние IP-адреса lnxsrv1 и lnxrtr1 вместо 32.54.87.114 32.54.87.115 /
    - Избегайте использования DNS-сервера в качестве определителя для любого имени домена в Интернете за исключением собственного домена. Например, если клиент в Интернете делает запрос для IP-адреса, скажем, www.google.com, то DNS-сервер не будет выполнять запрос к нему, но сделает его для www.site4you.kz.
      * Для запросов от внутренних клиентов, он будет выполняться, независимо от доменного имени.
      * Пользователи не должны быть в состоянии открыть вредоносные веб-сайты.
      * Пользователь должен быть перенаправлен на страницу перехода, размещенную на lnxsrv1.
        + Страница перехода должна отображаться следующее сообщение:  
          *«ВНИМАНИЕ: Сайт, который Вы пытаетесь посетить был отмечен как вредоносный, поэтому доступ к нему был запрещен»*
      * Вредоносные домены:
        + download.malware.com
        + abcd.bad.net
        + dangerous.org
        + site.is.malicious.net
        + virus1.net - virus10.net
  + FTP (proftpd)
    - Включить FTPS
      * Использовать сертификат, подписанный lnxsrv2
      * Использовать скрытное шифрование
    - Создать учетную запись пользователя FTP для каждого сайта веб-сервера
      * Пользователь «site4you» с паролем «Skills39»
      * Пользователь «intranet» с паролем «Skills39»
    - Убедиться, что пользователи заперты в соответствующей директории корневого каталога документов сайта.
    - Убедиться, что возможна передача файлов на сервер.
  + Почта
    - Вы можете использовать любое программное обеспечение для почтового сервера. Будет применяться функциональное тестирование.
    - Убедитесь, что пользователи от user20 дл user30 имеют доступ через IMAPS и SMTPS
    - Использовать сертификаты, подписанные lnxsrv2 для SSL/TLS шифрования
    - Использовать аутентификацию по сертификату клиента в дополнение к сервисам IMAP и SMTP
    - Создать список рассылки it@site4you.kz
      * пользователи от user20 до user29 должны быть в списке рассылки
    - пользователю user21 не разрешается отправлять электронные сообщения (через SMTP)
    - До окончания вашего проекта убедиться, что вы отправили электронное сообщение пользователям от user20 до user30 и другое сообщение от user30 до user20. Отправить сообщение также от пользователя user20 в списке рассылки
    - Не удалять эти сообщения

## РАБОЧЕЕ ЗАДАНИЕ СЕРВЕР lnxsrv2

Примечание: Пожалуйста, используйте конфигурацию по умолчанию, если вам не предоставили подробной информации.

* Настроить сервер с именем узла, доменом и IP-адресом, указанным в приложении.
* Установить службы
  + Совместный доступ к файлам (Samba)
    - Предоставить доступ к папке «internal»
      * Путь: /data/internal
      * Предоставить доступ только для пользователей от «user1» до «user10»
      * Убедиться, что совместный доступ не отображается в сети браузере клиентов
    - Предоставить доступ к папке «public»
      * Путь: /data/public
      * Включить доступ только для чтения для всех
  + CA (openssl)
    - Настроить как CA
    - Атрибуты CA должны быть установлены следующим образом
      * Код страны: KZ
      * Организация: Site4you
    - Создать корневой СА сертификат
    - Хранить все файлы, относящиеся к CA в /ca и убедиться, что ключ CA доступен только корню. (Вам разрешается расположить все в /ca или использовать подпапки в /ca)

# ЧАСТЬ А2

## РАБОЧЕЕ ЗАДАНИЕ УСТАНОВКА (LNXCLNT1, LNXCLNT2)

Примечание: Пожалуйста, используйте конфигурацию по умолчанию, если вам не предоставили подробной информации.

## РАБОЧЕЕ ЗАДАНИЕ LNXCLNT1

Примечание: Пожалуйста, используйте конфигурацию по умолчанию, если вам не предоставили подробной информации.

* Установить базовую ОС и использовать Gnome для GUI.
* Настроить клиента с именем узла, доменом и IP-адресом, указанным в приложении
* Убедиться, что клиент может подключиться к lnxsrv2 (через lnxrtr1) через VPN
* Убедиться, что корневой СА сертификат lnxsrv2 надежный
* Убедиться, что сертификат клиента установлен
* Установить клиент FileZilla FTP
* Установить почтовый клиент Icedove
  + Настроить почтовый ящик пользователя user20
  + Убедиться, что пользователь user20 может отправлять письма пользователю user30
* Убедиться, что клиент может получить совместный доступ к файлам samba.

## РАБОЧЕЕ ЗАДАНИЕ LNXCLNT2

Примечание: Пожалуйста, используйте конфигурацию по умолчанию, если вам не предоставили подробной информации.

* Установить базовую ОС и использовать Gnome для GUI
* Настроить клиента с именем узла, доменом и IP-адресом, указанным в приложении
* Убедиться, что корневой СА сертификат lnxsrv2 надежный
* Убедиться, что сертификат клиента установлен
* Установить почтовый клиент Icedove
  + Настроить почтовый ящик пользователя user30
  + Убедиться, что пользователь user30 может отправлять письма пользователю user20
* Убедиться, что клиент может получить внутренний совместный доступ к файлам.
* Установить Cadaver (клиент WebDAV)

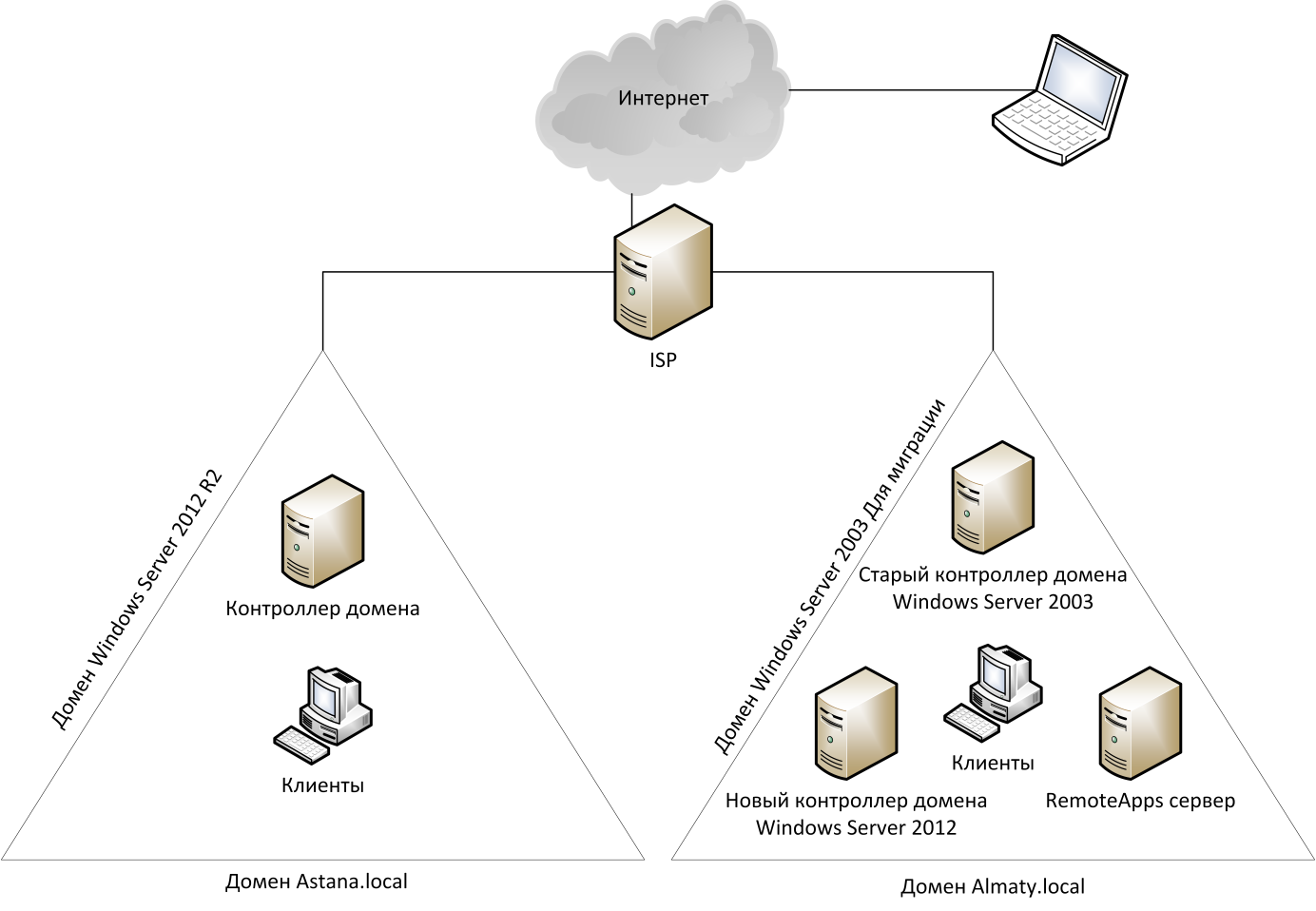
# модуль B - среда Windows

## ОПИСАНИЕ ПРОЕКТА И ЗАДАНИЙ

Вас наняла на работу в качестве внешнего IT-консультанта компания под названием Skills39, расположенная в Астане. В июле Skills39 выкупила другую компанию, расположенную в Алматы.

Ваша задача заключается в интеграции и перемещении компании в Алматы в Skills39. Вы также должны реализовать решение для удаленного доступа для персонала из сферы продаж, чтобы они могли подключаться к сети компании. Во внутренней сети вы должны сосредоточить некоторые приложения и реализовать некоторые удаленные приложения RemoteApps для особой группы сотрудников.

## Краткая спецификация



## ЧАСТЬ 1 *(установка ISP сервера)*

**ПРИМЕЧАНИЕ: Пожалуйста, используйте конфигурацию по умолчанию, если вам не предоставили подробной информации**

### РАБОЧЕЕ ЗАДАНИЕ I-ISP сервер

* Сервер уже предварительно установлен (Windows Server 2012 R2 с GUI)
* Настроить сервер с параметрами, заданными в схеме в конце документа
* **НЕ** подключать сервер к любому домену, оставить сервер в рабочей группе
* Назвать эту рабочую группу «ISP»

### маршрутизациЯ и межсетевой защитный экран

Установить и настроить службы LAN-маршрутизации

* Перенести трафик из сети интернет (143.25.0.0) к сети Almaty и Astana, а также в обратном направлении
* Разрешить весь трафик между сетью Almaty и Astana

### DNS (для сети интернет 143.25.0.0/25)

Установить и настроить службу DNS

* Служба DNS должна быть только на интерфейсе 143.25.0.1
* создать необходимые передовые зоны
* создать А-записи для следующих узлов:
  + da.skills39.net --> 143.25.0.20
  + www.msftncsi.com --> 143.25.0.1
  + dns.msftncsi.com --> 131.107.255.255
* создать для каждой подсети зону обратного просмотра

### DHCP (для сети интернет 143.25.0.0/24)

Установить и настроить службу DHCP

* Диапазон 143.25.0.150 – 143.25.0.160/24 (Интернет-Клиенты)
* Шлюз по умолчанию 143.25.0.1
* DNS сервер 143.25.0.1
* Служба должна быть только на серверах Интернет интерфейса (143.25.0.1)

### IIS

Установить и настроить IIS службу

* Создать веб-сайт для www.msftncsi.com
* Создать в корневой папке веб-сайта файл с именем «ncsi.txt»
  + Содержание этого файла должно быть: Microsoft NCSI (**не нажимайте enter в конце**)
* Проверьте веб-сайт http://www.msftncsi.com/ncsi.txt
  + Должен отображать **Microsoft NCSI**

## ЧАСТЬ 2 *(установка домена astana.local)*

**ПРИМЕЧАНИЕ: Пожалуйста, используйте конфигурацию по умолчанию, если вам не предоставили подробной информации**

### РАБОЧЕЕ ЗАДАНИЕ AS-DC сервер

* Сервер уже предварительно установлен (Windows Server 2012 R2 с GUI)
* Настроить сервер с параметрами, заданными в схеме в конце документа
* Изменить правила брандмауэра по умолчанию для разрешения трафика ICMP (пинг)
* Добавить дополнительный виртуальный жесткий диск (5 Гб), как D: диск

#### Служба каталогов ActiveDirectory

* Установить и настроить службу доменов Active Directory для **Astana.local**
* Создать следующие глобальные AD группы:
  + AS-SalesUser
  + AS-MktUser
  + AS-ITUser
  + AS-HRUser
  + AS-AcctUser
  + AS-Visitor
  + AS-Manager
* Создать учетные записи пользователей, согласно списку в приложении 1.
  + Система основных имен пользователей определяются политикой компании как «logon@skills39.net»
  + Все пользователи должны быть включены и пароль не должен быть изменен при первом входе
  + Добавить пользователей в обязательную группу

#### DNS

Установить и настроить службу DNS

* Создать также обратную зону для внутренней подсети
* Создать статические A-записи для всех серверов

#### DHCP

Установить и настроить службу DHCP

* Диапазон 172.16.10.150 – 172.16.10.180/24 (Клиенты)
* Шлюз по умолчанию 172.16.10.1
* DNS сервер 172.16.10.10

#### PKI

Установить и настроить службу сертификатов

* Установить только «Источник сертификатов»
* Создать маску для клиентов и серверов
  + Назвать маску «Skills39-ClientServerCert»
  + Поместить маску в Active Directory
  + Установить формат названия темы на «общее название»

#### GPO

Установить и настроить интеллектуальное централизованное управление

* Установить следующие настройки
  + Все пользователи должны получить читаемый баннер при входе
    - Название: «Добро пожаловать в Skill39»
    - Сообщение: «Разрешен доступ только авторизованному персоналу»
    - Запретить это сообщение на всех серверах!!!
  + Автоматическое включение сертификата «Skills39-ClientServerCert» для всех клиентов и серверов
  + Включить пользователей AS-ITUsers в локальную группу администраторов на всех клиентах ОС Windows 8.1
  + Отключить использование команд «cmd» и «run» для группы AS-Visitor
  + Отключить «Анимацию при первом входе» для всех клиентов ОС Windows 8.1
  + Скрыть все локальные диски для группы AS-Visitor
  + Создать подробную политику для паролей, требующую 7-символьные несложные пароли для обычных пользователей, 8-символьные сложные пароли для членов группы AS-ITUser
    - Отключить «соблюдение минимального срока действия пароля»
  + Все пользователи (кроме AS-ITUsers) в Астане должны иметь ограниченные утилиты для редактирования реестра

#### файловая служба

Настроить пользовательские профили, домашние диски и общие папки

* Домашние папки
  + Создать Домашнюю папку для каждого пользователя
  + Локальный путь на сервере **d:\users\homes\%username%**
  + Связать Домашнюю папку автоматически с диском H: [**\\AS-DC.astana.local\homes\%username%**](file:///\\S-DC.saopaulo.local\homes\%25username%25)
  + Выделить объём памяти для каждой папки домашнего диска в 20Мб
* Перемещаемые профили
  + Локальный путь на сервере d:\users\profiles\%username%
  + Создать перемещаемые профили для всех пользователей   
    \\AS-DC.astana.local\profiles\%username%
* Общие папки отделов
  + Локальный путь на сервере
    - d:\shares\HR
    - d:\shares\IT
    - d:\shares\Sales
    - d:\shares\Mkt
    - d:\shares\Acct
  + Все пользователи должны иметь разрешение на ЧТЕНИЕ других общих папок отделов (за исключением ACCT), ИЗМЕНЕНИЕ для собственного отдела и ПОЛНЫЙ КОНТРОЛЬ для документов, которые они создают
  + Только пользователи AcctUsers должны видеть и иметь доступ к общей папке Acct
  + Автоматически связывать общую папку отдела (d:\shares) с диском S:   
    **\\AS-DC.astana.local\department**
  + Исключить **ТОЛЬКО** .exe и .cmd файлы в общих папках отделов

#### РАБОЧЕЕ ЗАДАНИЕ AS-Client

* Клиент уже предустановлен (Windows 8.1 Enterprise Edition)
* Настроить клиент с параметрами, заданными в схеме в конце документа
* Изменить правила брандмауэра по умолчанию для разрешения ICMP (пинг) трафика
* Установить локальный пароль администратора на **Astana16**
  + Включить локальную учетную запись администратора
* Подключить компьютер к домену astana.local
* Изменить настройку питания, чтобы клиент никогда не переходил в режим ожидания во время подключения
* Использовать этот клиент для тестирования входа пользователя в систему, профилей, домашнего диска и настроек GPO

## ЧАСТЬ 3 *(клиент в Интернет)*

ПРИМЕЧАНИЕ: Пожалуйста, используйте конфигурацию по умолчанию, если вам не предоставили подробной информации

### РАБОЧЕЕ ЗАДАНИЕ AS-Remote

* подключить клиента к внутренней сети
  + Этот клиент уже установлен заранее (Windows 8.1 Enterprise Edition)
  + Настроить клиент с параметрами, заданными в схеме в конце документа
  + Изменить правила брандмауэра по умолчанию для разрешения ICMP (пинг) трафика
  + Установить локальный пароль администратора на **Astana16**
    - Включить локальную учетную запись администратора

## ЧАСТЬ 4 *(перемещение домена almaty.local)*

ПРИМЕЧАНИЕ: Пожалуйста, используйте конфигурацию по умолчанию, если вам не предоставили подробной информации

### РАБОЧЕЕ ЗАДАНИЕ AL-DC1 и AL-DC2

Ваше задание заключается в том, чтобы переместить совокупность деревьев almaty.local на тот же уровень, что и в astana.local.

Использовать «WorldSkills2016» для входа в AL-DC2

#### СЛУЖБЫ КАТАЛОГОВ

* Установить новый контроллер домена (AL-DC1). Вы должны установить этот сервер с нуля с операционной системой «Windows Server 2012 R2»
* Настроить сервер с параметрами, заданными в схеме в конце документа
* Установить функциональные уровни домена и совокупности деревьев 2012 R2
* Переместить все роли на новый сервер
* Правильно удалить сервер 2003 из домена
* Удалить DHCP и DNS службу
* Создать условное перенаправление с astana.local
* Создать двухканальное доверие с almaty.local
* Создать AD группы AL-Sales и AL-Marketing и добавить соответствующих пользователей

#### DHCP СЛУЖБЫ

* Переместить все DHCP области на новый сервер
* Любая аренда, опция или резервирование могут не исчезнуть
* Изменить параметр DHCP для DNS сервера AL-DC1

#### Файловые службы

* Переместить все файлы из **\\AL-DC2\homes** и **\\AL-DC2\profiles** в новый DC (R-DC1)
  + Все разрешения на общий доступ или NTFS должны быть одинаковыми в новой общей папке
  + Общие папки для нового места должны быть **\\AL-DC1\homes** и **\\AL-DC1\profiles**
* Изменить пользователей для доступа к общим папкам напрямую из нового расположения (домашняя и профильная папки)

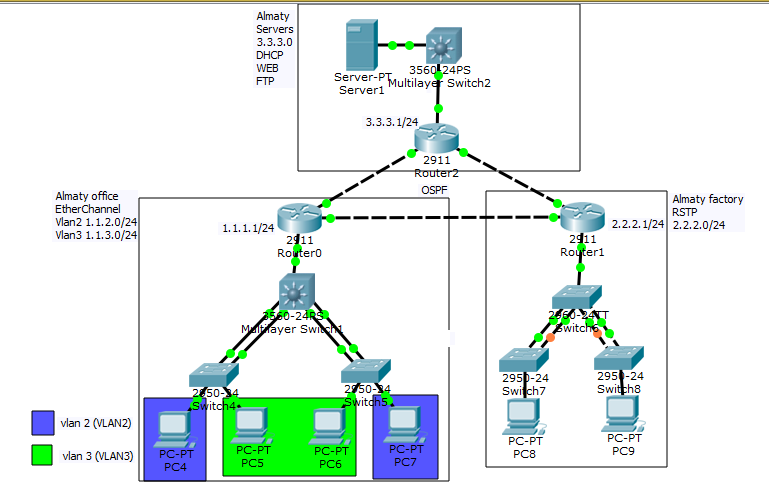
#### Web СЕРВЕР

* Переместить сайт http://intranet.almaty.local на новый сервер, так чтобы он реагировал на https://intranet.almaty.local

### РАБОЧЕЕ ЗАДАНИЕ AL-Client

* Этот клиент заранее не установлен. Вы должны установить его с нуля, с помощью операционной системы «Windows 8.1 Enterprise Edition»
  + Настроить клиент с параметрами, заданными в схеме в конце документа
  + Изменить правила брандмауэра по умолчанию для разрешения ICMP (пинг) трафика
  + Установить локальный пароль администратора на **Astana16**
    - Включить локальную учетную запись администратора
* Подключить компьютер к домену almaty.local
* Изменить настройку питания, чтобы клиент никогда не переходил в режим ожидания во время подключения
* Использовать этот клиент для тестирования пользователей Almaty (домашних и профильных)
* Отключить «Анимацию при первом входе»

# 3 модуль С - Cisco Packet Tracer



Almaty office:

Создать 2 vlan’a (VLAN2 и VLAN3)

ROUTER: 1.1.1.1/24

VLAN2: 1.1.2.0/24

VLAN3: 1.1.3.0/24

Любой трафик между VLAN2 и VLAN3 запрещён

Порты fa0/23-24 на свитчах второго уровня объединены по протоколу EtherChannel и подключаются к fa0/1-2 и fa0/3-4 L3 свитче

L3 свитч должен выполнять функцию маршрутизации для внутреннего трафика (в сети Almaty office)

Almaty factory:

ROUTER: 2.2.2.1/24

VLAN1: 2.2.2.0/24

Порты fa0/23-24 на свитчах второго уровня объединены по протоколу RSTP и подключаются к fa0/1-2 и fa0/3-4 на L3 свитче

Almaty servers:

ROUTER: 3.3.3.1/24

Server1: 3.3.3.11/24

Службы на Server1:

DHCP

WWW

FTP

Общее:

Настроить вход в привилегированный режим через по логину logcsico и паролю passcisco

Настроить протокол динамической маршрутизации OSPF

Все компьютеры должны получать IP адрес от DHCP сервера (Server1) соответственно указанным IP адресам vlan’ов

У всех пользователей должен быть доступ к на веб-сервер

У всех пользователей КРОМЕ пользователей VLAN3 в сети Almaty office должен быть доступ к FTP

Запрещён любой трафик между подсетями VLAN2 и VLAN3 в сети Almaty office

Проверка:

Пинг сервера из VLAN2 в сети Almaty office

Открытие web страницы Server1 из VLAN2 в сети Almaty office

Подключение к ftp Server1 из VLAN2 в сети Almaty office

Пинг компьютера в VLAN3 с компьютера VLAN2 (не должен проходить)

Пинг сервера из VLAN3 в сети Almaty office

Открытие web страницы Server1 из VLAN3 в сети Almaty office

Подключение к ftp Server1 из VLAN3 в сети Almaty office (не должно быть доступа)

Пинг компьютера в VLAN2 с компьютера VLAN3 (не должен проходить)

Пинг сервера из сети Almaty factory

Подключение к ftp Server1 из сети Almaty factory

Пинг VLAN2 и VLAN3 (Almaty office) из сети Almaty factory

Пинг сети Almaty factory из VLAN2 и VLAN3 (Almaty