2.1. Заключительный тур олимпиады

Часть 1

Настроить оборудование в лабораторной среде Packet Tracer

Топология

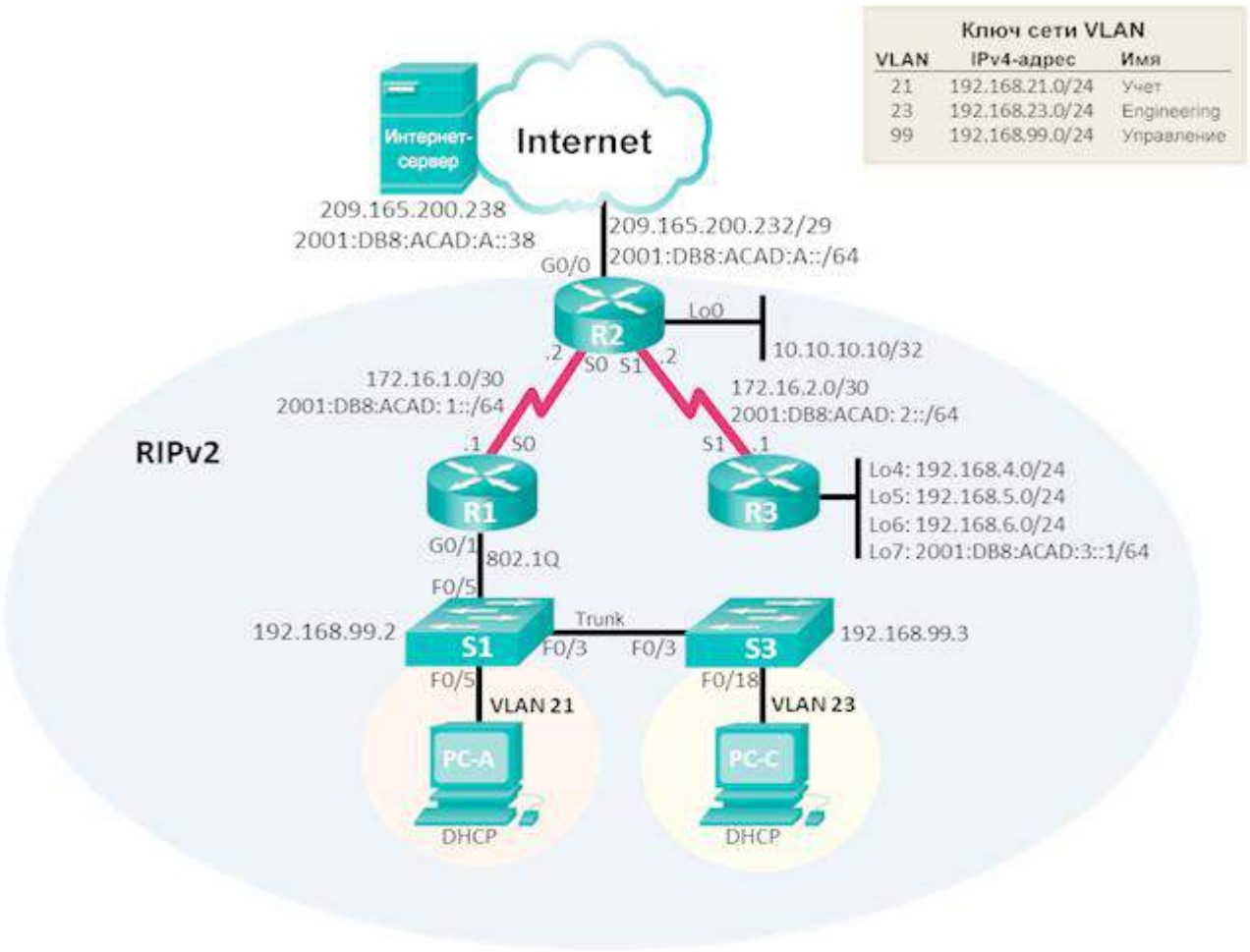


Схема 1

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941).
- 2 коммутатора (Cisco 2960).
- 3 ПК
- кабели Ethernet и последовательные кабели в соответствии со схемой 1

1. Вам необходимо настроить проект сети в лабораторной среде Cisco PT согласно схемы 1, соблюдая следующие требования

2. Все пароли должны содержать слово ior, их необходимо будет сохранить на рабочем столе в файле pass.txt

3. Пароли не должны отображаться в открытом виде при просмотре конфигурации устройств

4. Пароль от привилегированного режима должен храниться в результате хэш-функции

5. Настроить сообщение дня с текстом «Unauthorized access is prohibited»

6. Обновления маршрутизации не должны передаваться в тупиковые сети

7. Компьютеры в сетях VLAN 21 и VLAN 22 должны автоматически получать адреса по протоколу DHCP

8. Настройте веб-сервер. Компьютеры должны заходить на сервер по имени iorskills2018.com

9. При входе на веб-сервер пользователи должны видеть страницу с краткой историей развития отечественной вычислительной техники

10. Обеспечьте безопасное удаленное управление всеми сетевыми устройствами

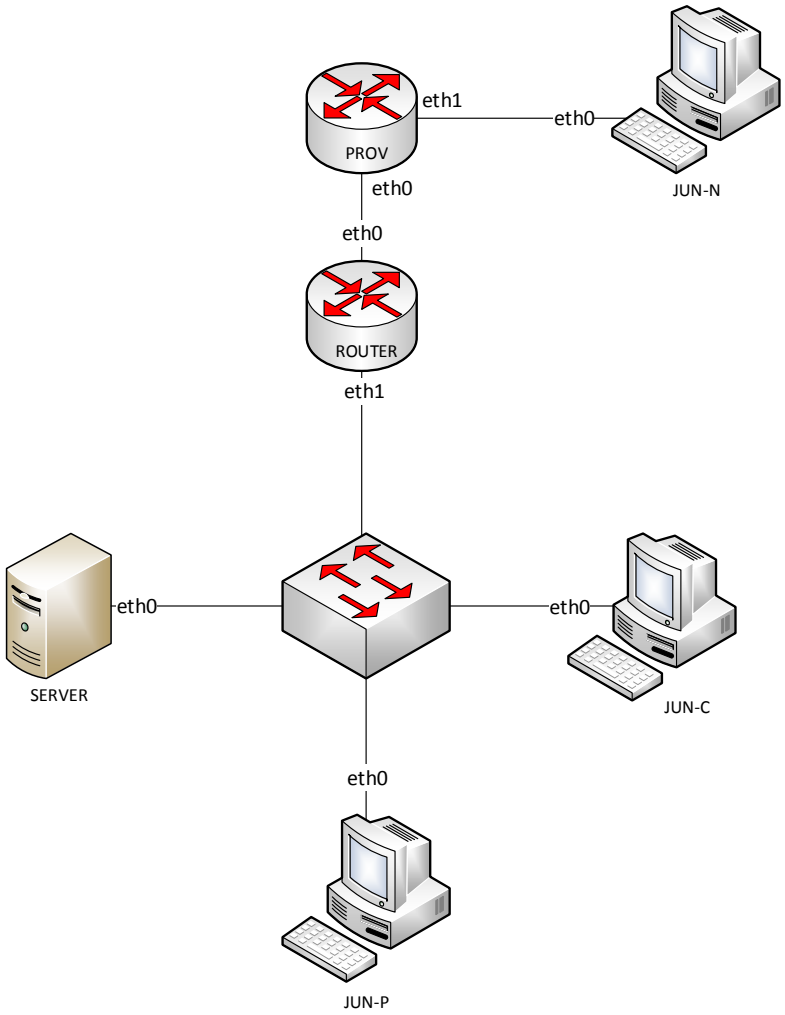
11. Настройте протокол маршрутизации (расчет метрики должен происходить только на основе количества переходов), сети не должны суммироваться, информация о сетях должна передаваться на адрес многоадресной рассылки.

12. Настроить службу NAT, на маршрутизаторе R2 (Пул адресов: 209.165.200.233 – 209.165.200.237)

13. Настроить дату и время на маршрутизаторе R2. R2 должен быть сервером NTP, остальные сетевые устройства должны быть клиентами NTP

Часть 2.

Схема 2



Виртуальные машины развернуты на сервере ESXI. Вам необходимо будет пользоваться клиентом ESXI

Конфигурация хостов

1) Настройте имена хостов в соответствии с **Таблицей 1.**
2) Установите следующее ПО на **ВСЕ** хосты:
    a. Пакет tcpdump
    b. Пакет net-tools
    c. Редактор vim

3) На хостах ROUTER, JUN-P, SERVER, JUN-N, JUN-C сформируйте файл **/etc/hosts** в соответствии с **Таблицей 1** (кроме адреса хоста JUN-P). Данный файл будет применяться во время проверки в случае недоступности DNS-сервисов. Проверка по IP-адресам выполняться не будет. В случае корректной работы DNS-сервисов изменения в файлах **/etc/hosts** не требуются.

Конфигурация сетевой инфраструктуры

1) Настройте IP-адресацию на ВСЕХ хостах в соответствии с **Таблицей 1.**
2) Настройте сервер протокола динамической конфигурации хостов для машин JUN-C и JUN-P
    a. В качестве DHCP-сервера используйте машину SERVER
    b. Используйте пул адресов 172.16.100.60 — 172.16.100.75
    c. Используете адрес машины SERVER в качестве адреса DNS-сервера
    d. Настройте DHCP-сервер таким образом, чтобы машина JUN-C всегда получала фиксированный IP-адрес в соответствии с **Таблицей 1**
    e. В качестве шлюза по умолчанию используйте адрес интерфейса ROUTER в локальной сети
    f. Используйте DNS-суффикс **juniormsk2018.com**
    g. DNS-записи типа A соответствующего хоста должны обновляться при получении им адреса от DHCP-сервера.

3) На машине SERVER настройте службу разрешения доменных имен
    a. Сервер должен обслуживать зону **juniormsk2018.com**
    b. Сопоставление имен организовать в соответствии с **Таблицей 2**
    c. Реализуйте поддержку разрешения обратной зоны.
    d. Файлы зон располагать в **/opt/dns/**

4) На ROUTER настройте интернет-шлюз для организации коллективного доступа в интернет. Настройте трансляцию сетевых адресов из внутренней сети в адрес внешнего интерфейса.

Службы централизованного управления и журналирования

1) На SERVER организуйте централизованный сбор журналов с хостов JUN-C, JUN-P и ROUTER.
    a. Журналы должны храниться в директории **/opt/logs/**
    b. Журналирование должно производится в соответствии с **Таблицей 3.**

Конфигурация служб удаленного доступа

1) На ROUTER настройте сервер удаленного доступа на основе технологии OpenVPN:
    a. В качестве сервера выступает ROUTER
    b. Параметры туннеля
        i. Устройство TUN
        ii. Протокол UDP
        iii. Применяется сжатие
        iv. Порт сервера 1122
    c. Ключевая информация должна быть сгенерирована на ROUTER
    d. Хранение всей необходимой (кроме конфигурационных файлов) информации организовать в **/opt/vpn**
2) На JUN-N настройте клиент удаленного доступа на основе технологии OpenVPN:
    a. Запуск удаленного подключения должен выполняться скриптом **start_vpn**
        i. Автоматизация отключения VPN-туннеля не требуется
        ii. Скрипт должен располагаться в **/opt/vpn**.
        iii. Скрипт должен вызываться из любого каталога без указания пути

iv. Используйте следующий путь для расположения файла скрипта **/opt/vpn/start_vpn.sh**

3) На ROUTER настройте удаленный доступ по протоколу SSH:
   a. Доступ ограничен пользователями **ssh_p** и **ssh_c**
   b. SSH-сервер должен работать на порту **1022**
4) На JUN-N настройте клиент удаленного доступа SSH:
   a. Доступ к серверу ROUTER должен происходить автоматически по правильному порту, без его явного указания номера порта в команде подключения
   b. Для других серверов по умолчанию должен использоваться порт **22**
   c. Доступ к ROUTER под учетной записью **ssh_p** должен происходить с помощью аутентификации на основе открытых ключей.

Конфигурация служб хранения данных

1) На SERVER настройте сервер файлового хранилища на основе технологии NFS:
   a. В качестве хранилища используется каталог **/opt/nfs**
   b. Доступ организуется для чтения и записи
2) Настройте автоматическое монтирование NFS-хранилища для клиентов JUN-C, JUN-P и JUN-N:
   a. Используйте DNS-имя NFS-сервера
   b. Используйте **/opt/nfs** в качестве пути для монтирования
   c. Клиенты JUN-C и JUN-P монтируют NFS-каталог при запуске ОС
   d. Клиент JUN-N монтирует NFS-каталог после установления VPN-туннеля с ROUTER

Конфигурация параметров безопасности и служб аутентификации

1) Настройте межсетевой экран на ROUTER
   a. Разрешите удаленные подключения с использованием OpenVPN на внешний интерфейс маршрутизатора ROUTER
   b. Разрешите SSH подключения на соответствующий порт

Таблица 1. Адресация

Сеть	**Хосты**	**Адреса (/24)**
Internal	JUN-P JUN-C ROUTER SERVER	DHCP 172.16.100.50 (DHCP) 172.16.100.1 172.16.100.100
Last Mile	PROV ROUTER	10.10.10.1 10.10.10.10
First Mile	PROV JUN-N	20.20.20.1 20.20.20.10

Таблица 2. DNS-имена

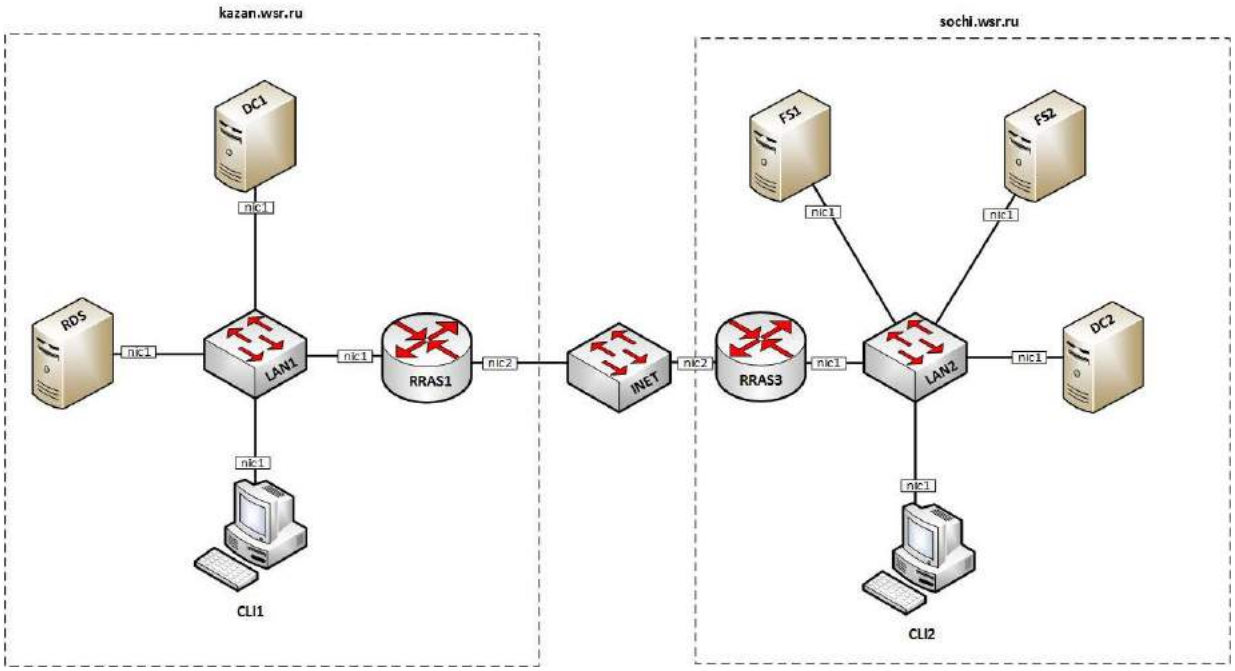
Хост	**DNS-имя**
JUN-P	A:JUN-p.juniormsk2018.com

	CNAME: mom.juniormsk2018.com CNAME: dad.juniormsk2018.com
JUN-C	A:JUN-c.juniormsk2018.com CNAME: son.juniormsk2018.com
SERVER	A:SERVER.juniormsk2018.com CNAME: server.juniormsk2018.com CNAME: center.juniormsk2018.com
ROUTER	A:ROUTER.juniormsk2018.com CNAME: fw.juniormsk2018.com

Таблица 3. Правила журналирования

Источник	**Уровень журнала**	**Файл**
Все хосты	critical и выше	/opt/logs/<HOSTNAME>/crit.log
SERVER	auth.*	/opt/logs/<HOSTNAME>/auth.log
ROUTER	*.err	/opt/logs/<HOSTNAME>/error.log
Все кроме ROUTER	*.err	/opt/logs/err.log

Часть 3.



Базовая настройка

1. Проверьте и по необходимости настройте базовые параметры на всех виртуальных машинах согласно таблице 1. При первом доступе к операционным системам либо следуйте указаниям мастера, либо, при необходимости, используйте следующие реквизиты: Administrator/Pa$$w0rd для серверных операционных систем, и User/Pa$$w0rd – для клиентских. Используемые логины и пароли сейчас и в дальнейшем документируйте. Обеспечьте наличие соответствующего документа на рабочем месте.
2. Настройте разрешения файловой системы

a. В домене kazan.wsr.ru на компьютере CLI1 предполагается использование файлов справки в формате .hlp. Для корректной работы справки найдите и удалите файл WinHlp32.exe. В дальнейшем вместо него будет использована нужная утилита.
b. Настройте на CLI1 общую папку *Distr*. Обеспечьте полный доступ к ней и к ее содержимому для доменных администраторов; члены группы *IT* должны иметь возможность добавлять, изменять и удалять содержимое папки, но не должны иметь возможность удалить саму папку *Distr*; члены группы *Sales* должны иметь возможность просматривать содержимое папки и открывать файлы, но им должно быть запрещено удалять что-либо из содержимого папки. Все настройки должны быть выполнены с учетом правила предоставления наименьших необходимых привилегий.

3. Настройте отказоустойчивость дисковой подсистемы
   a. В домене sochi.wsr.ru на сервере FS1 настройте программное зеркалирование системного диска. Используйте для этого один из имеющихся в составе сервера дополнительных дисков. Вносить изменения в настройки виртуальной машины при этом запрещается! Будьте внимательны, переразметить системный раздел после зеркалирования не удастся, поэтому можете использовать второй из имеющихся дополнительных на сервере дисков для создания резервных копий.

Настройка сетевых служб

1. На серверах RRAS1, RRAS3 разверните соответствующие роли для обеспечения возможностей маршрутизации и удаленного доступа.
2. Настройте протокол динамической маршрутизации RIP между офисами kazan.wsr.ru и sochi.wsr.ru.
3. На серверах RRAS1, RRAS3 разверните роль для динамической выдачи IP-адресов и других сетевых настроек клиентам соответствующих сетей, и настройте пулы адресов в соответствии с таблицей 2. Учтите, что при получении IP-адреса компьютеры должны автоматически регистрироваться в базе DNS соответствующего домена.
4. Переведите клиентские компьютеры в обоих офисах в режим автоматического получения сетевых настроек. Убедитесь в правильности полученных настроек.

Настройка служб каталогов

1. На сервере DC1 установите роль контроллера домена kazan.wsr.ru. В процессе установки так же установите роль DNS-сервера и настройте соответствующие зоны.
2. На сервере DC2 установите роль контроллера домена sochi.wsr.ru. В процессе установки так же установите роль DNS-сервера и настройте соответствующие зоны.
3. Создайте пользователей, группы и организационные подразделения в доменах согласно таблице 3. Учтите, что создавать каждого пользователя вручную накладно, используйте соответствующий скрипт. Все созданные учетные записи пользователей должны быть включены и иметь пароль P@ssw0rd

4. Между доменами kazan.wsr.ru и sochi.wsr.ru установите односторонние доверительные отношения: пользователи домена kazan.wsr.ru должны иметь доступ к ресурсам домена sochi.wsr.ru (без дополнительных настроек в AD и DNS), но не наоборот.
5. На серверах DC1 и DC2 настройте пересылку DNS-запросов между доменами kazan.wsr.ru и sochi.wsr.ru. При появлении новых DNS-серверов они должны получать соответствующие настройки автоматически.
6. Введите компьютеры RDS, CLI1, RRAS1 в домен kazan.wsr.ru.
7. Введите компьютеры FS1, FS2, CLI2 и RRAS3 в домен sochi.wsr.ru.
8. В домене kazan.wsr.ru настройте групповые политики, обеспечивающие выполнение следующих условий (используйте значащие имена создаваемых политик):
    a. пользователи группы *Group1* должны быть членами локальных групп администраторов на всех компьютерах данного домена;
    b. для всех пользователей домена при открытии браузера *IE* должна открываться стартовая страница терминального сервера.
9. В домене sochi.wsr.ru настройте групповые политики, обеспечивающие выполнение следующих условий (используйте значащие имена создаваемых политик):
    a. удаленный рабочий стол включен на всех компьютерах домена и доступен для администраторов домена;
    b. для всех пользователей домена включено перенаправление папок *Desktop* и *MyDocuments* на файловый сервер FS1 в специально созданные для этого папки (задокументируйте пути к этим папкам);
    c. сетевые папки *Man_share* и *Work_share* с файлового сервера FS2 подключены как сетевые диски (Z:\) для пользователей групп *Managers* и *Workers* соответственно;
10. В домене sochi.wsr.ru для членов группы *Managers* настройте перемещаемые профили. Для хранения профилей создайте папку *D:\Profiles* на сервере FS2.
11. Проследите за тем, чтобы пользователь имел полный доступ к файлам своего профиля на сервере и не имел никакого доступа к файлам профилей других пользователей.

Настройка общих служб

1. На сервере RDS установите и настройте роль терминального сервера.
2. На сервере DC1 установите и настройте роль удостоверяющего центра с названием *MainCA*.
3. Разверните терминальный сервер с лицензированием по компьютерам (используйте временную лицензию).
4. Сконфигурируйте web-доступ RemoteApp к службам терминалов сервера.
5. Опубликуйте программу *Wordpad* на web-портале RemoteApp для членов группы *IT*.
6. Опубликуйте программу *Notepad* на web-портале RemoteApp для членов группы *Sales*.
7. Web-интерфейс сервера должен быть настроен таким образом, чтобы пользователи могли автоматически получать доступ к форме входа на web-интерфейс удаленных рабочих столов при указании адресов http://rds.kazan.wsr.ru и https://rds.kazan.wsr.ru.
8. С помощью доменного центра сертификации на сервере CA сгенерируйте и используйте для терминальных служб соответствующий SSL-сертификат. Сертификат

должен быть использован для всех установленных компонентов терминальных служб. При обращении с любого компьютера в домене kazan.wsr.ru к сайту по имени https://rds.kazan.wsr.ru сертификат должен распознаваться как доверенный и действительный.

Настройка служб управления файловыми хранилищами

1. В домене sochi.wsr.ru на серверах FS1 и FS2 установите соответствующие роли для организации распределенной файловой системы.
2. Создайте папку *C:\Share* на сервере FS1 и папку *D:\Share* на сервере FS2. Внутри созданных папок создайте папки *Man_share* и *Work_share*.
3. Создайте корень DFS с именем *FS*. Данный корень должен поддерживаться обоими серверами. Создайте под этим корнем папку с именем *Share*, ссылающуюся на сетевые директории с тем же именем (Share) созданные вами ранее на каждом сервере. Обеспечьте всем пользователям домена доступ к этой папке на запись. Настройте репликацию между папками средствами DFS. Установите жесткое ограничение 1 Гб на размер папки *FS\Share*.
4. Запретите хранение аудио- и видео-файлов в папках *Share* на серверах FS1 и FS2.
5. Установите на сервере FS2 файловые квоты согласно таблице 4.

Таблица 1. Базовая настройка.

№ п/п	Имя компьютера	Основной DNS-суффикс	IP-адрес	Имя локального администратора/пароль
1	DC1	kazan.wsr.ru	10.10.10.10/24	admin/P@ssw0rd
2	RDS	kazan.wsr.ru	10.10.10.50/24	
3	CLI1	kazan.wsr.ru	10.10.10.62/24	
4	RRAS1	kazan.wsr.ru	nic1: 10.10.10.1/24 nic2: 20.17.255.1/29	
5	DC2	sochi.wsr.ru	10.20.20.10/24	
6	FS1	sochi.wsr.ru	10.20.20.20/24	
7	FS2	sochi.wsr.ru	10.20.20.30/24	
8	CLI2	sochi.wsr.ru	10.20.20.63/24	
9	RRAS3	sochi.wsr.ru	nic1: 10.20.20.1/24 nic2: 20.17.255.3/29	

Таблица 2.Диапазоны адресов.

№ п/п	Офис	Начальный адрес	Конечный адрес	Исключения
1	kazan.wsr.ru	10.10.10.100/24	10.10.10.180/24	10.10.10.150

2	sochi.wsr.ru	10.20.20.70/24	10.20.20.90/24	-

Таблица 3. Доменная иерархия.

№ п/п	Домен	Подразделение	Группа	Члены группы
1	kazan.wsr.ru	Employees	Sales	User1, …, User20
2	kazan.wsr.ru	Employees	IT	User30, …, User40
3	kazan.wsr.ru		VPN_Users	IT
4	kazan.wsr.ru		Group1	User21,…, User29
4	sochi.wsr.ru	Office	Workers	User1, …, User15
5	sochi.wsr.ru	Office	Managers	User16, …, User30
6	sochi.wsr.ru		Admins	Admin1

Таблица 4. Файловые квоты.

№ п/п	Путь	Тип квоты/размер	Уведомление	Отчет пользователю
1	D:\Share\Man_share	Жесткая/300 Mb	по e-mailпри 85% и 100%	о дублирующих файлах
2	D:\Share\Work_share	Срасширением/ 200Mb+50Mb	поe-mailпри 100%	обольшихфайлах