МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

кафедра Компьютерных технологий

«Допущен к защите»
Заведующий кафедрой КТ
(Ф.И.О., ученая степень, звание)
(подпись) «_____» _____ **20__ г.**

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Проектирование корпоративной сети с подключением к двум провайдерам

Специальность Вычислительная техника и программное обеспечение

Выполнил (а) Ашимов Куаныш Ермаханович БВТ-10-3
(Фамилия и инициалы) группа

Научный руководитель Тайгожекова А. Ж., ст. препод.
(Фамилия и инициалы, ученая степень, звание)

Консультанты:

по экономической части:
Ерешева З.Д., асс. преподаватель
(Фамилия и инициалы, ученая степень, звание)
Ерешева «20» 05 2014 г.
(подпись)

по безопасности жизнедеятельности:
Трифонова Н.Г. д.х.н., профессор
(Фамилия и инициалы, ученая степень, звание)
«06» 05 2014 г.
(подпись)

по применению вычислительной техники:
Тайгожекова А. Ж., ст. препод
(Фамилия и инициалы, ученая степень, звание)
«26» мая 2014 г.
(подпись)

(Фамилия и инициалы, ученая степень, звание)
«_____» _____ 20__ г.
(подпись)

Нормоконтролер: Тусупов Д.М.
(Фамилия и инициалы, ученая степень, звание)
«30» мая 2014 г.
(подпись)

Рецензент: Байбатшаев М.Ш., к.т.н., профессор
(Фамилия и инициалы, ученая степень, звание)
«2» 06 2014 г.
(подпись)

Алматы 2014 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Факультет Информационные технологии
Специальность Вычислительная техника и программное обеспечение
Кафедра Компьютерные технологии

ЗАДАНИЕ
на выполнение дипломного проекта

Студент Ашимов Куаныш Ерланович
(фамилия, имя, отчество)
Тема проекта Проектирование корпоративной сети с подключением к двум провайдерам

утверждена приказом ректора № 115 от «24» сентября 2013 г.
Срок сдачи законченной работы «___» июнь 2014 г.
Исходные данные к проекту требуемые параметры результатов проектирования (исследования) и исходные данные объекта
книги по проектированию сетей

Перечень подлежащих разработке дипломного проекта вопросов или краткое содержание дипломного проекта:

Анализ предметной области
Теоретические аспекты проектирования корпоративной сети
Применение настроек конфигурации сети
Тестирование.

Перечень графического материала (с точным указанием обязательных чертежей)

Структура взаимодействия с серверами имен
Формат DNS - сообщений.

Рекомендуемая основная литература

Олифер В.Г., Олифер Н.А. Компьютерные сети

Консультанты по проекту с указанием относящихся к ним разделов

Раздел	Консультант	Сроки	Подпись
БЖД	Дроздова Н.Г.	11.04 – 26.05.14	
Экономика	Ерешева З.Д.	15.04 – 20.05.14	
Основная часть	Тайгозикова А.Ж.	11.04 – 26.05.14	
Нормоконтроль	Тусупов Д.М.	30.05.14г.	

Г Р А Ф И К
подготовки дипломного проекта

№ п/п	Наименование разделов, перечень разрабатываемых вопросов	Сроки представления руководителю	Примечание
	Анализ предметной области	26.04	
	Проектирование сети	09.05	
	Тестирование	10.05	

Дата выдачи задания «3» марта 2014 г.

Заведующий кафедрой _____ _____
(подпись) (Фамилия и инициалы)

Руководитель _____ Тайгожинова А.Н.
(подпись) (Фамилия и инициалы)

Задание принял к исполнению
студент _____ Аширов К.Е.
(подпись) (Фамилия и инициалы)

АҢДАТПА

Осы берілген дипломдық жобада аудың топологиясы қалааралық филиалдар үшін жасалуы қарыстырылған**.** Жұмыстың сипаттамаларының компьютерлік зерттеу мен сипаттау кезеңдерінен тұрады.

Мәліметті суреттеменің кеңістік шегіне енгізілу тәсілдерінің талдауы өткізілген. Жобада аудың бизнес-модель тиімділіктің және өтімділіктің мерзімінің көрсеткіштерімен қоса беріледі. Жұмыс қауіпсіздіктің және еңбектің күзетінің техникасының шаралары қарыстырылған.

АННОТАЦИЯ

В данном дипломном проекте рассматривается топология сети для филиалов. Разработка включает в себя этапы исследования, описания работы с компьютерными сетями.

Проведен анализ топологии сети и выбор различных протоколов. В проекте прилагается бизнес-модель сети с показателями эффективности и сроков окупаемости. Так же рассмотрены меры техники безопасности и охраны труда.

ANNOTATION

In this thesis project is considered for long-distance network topology branches. Development includes the steps of research, job descriptions with computer networks.

The analysis of network topology and the choice of different protocols. In the project business model attached network performance indicators and payback period. Just consider safety precautions and

Содержание

Введение

Персональные компьютеры – одна из самых важных частей современного мира, а компьютерные сети значительно облегчают нашу жизнь, ускоряя работу по обмену информацией, а также выходом в глобальную корпоративная сеть.

Сегодня можно с уверенностью сказать, что компьютерные сети стали занимать значительную часть в нашей жизни, а область их применения захватывает огромную долю большинства сфер деятельности человека.

Размеры компьютерных сетей могут существовать различных размеров – от несколько соединенных между собой в корпоративная сеть компьютеров, до несколько тысяч компьютеров, расположенных в разных частях света.

Целью данного проекта является проектирование корпоративной компьютерной сети для филиала компании. В работе описаны и применены такие технологии и протоколы как DHCP, OSPF, NAT. Для обеспечения стабильного функционирования сети, корпоративная сеть должна иметь надёжностью кабельных соединения, правильной топологией, правильным выбором мест расположения оборудования. Созданная корпоративная корпоративная сеть должна позволить обеспечить коллективный доступ в Интернет, что позволяет иметь возможность сотрудникам проводить аудио – видео конференции. При этом важно обеспечить низкий бюджет проекта, чтобы сохранить доступность подключения. В данной работе проработаны все решения построения современной, качественной корпоративной сети. Примененные нами технологии позволяют говорить о правильности технических решений в виде стабильной, работоспособной сети филиала.

1. Задание к проектированию

В эмуляторе необходимо создать проект корпоративной сети изображенной на рисунке 1.1. Использовав IP-адресацию разделить корпоративную сеть на необходимые подсети и установить необходимые настройки для всех устройств. Настроить маршрутизацию между всеми подсетями. Поднять и настроить протоколы динамической маршрутизации OSPF. Произвести настройку DNS и HTTP-серверов. Раздачу IP-адресов, производить с помощью DHCP. Использовать технологию NAT.

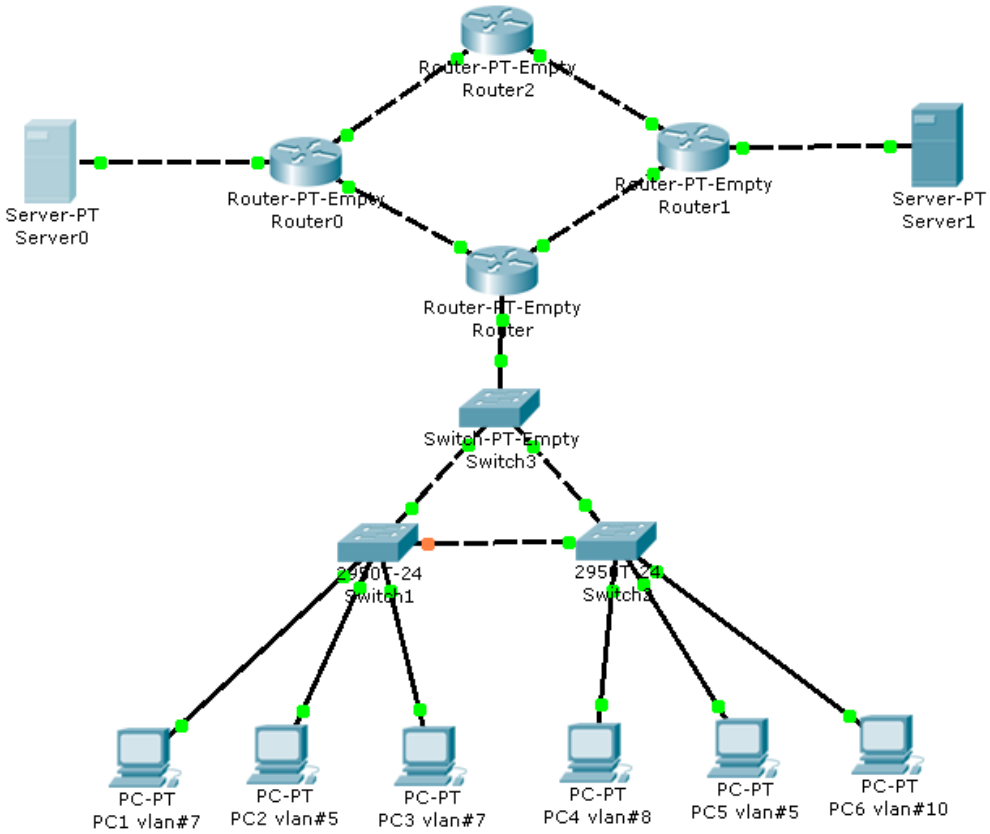

Рисунок 1.1 - Проектируемая корпоративная сеть

Рассчет сети

В соответствии с заданием на проектирование адресное пространство 192.168.1.0/24, которое надо разделить на 4 подсети(vlan_1-vlan_4).

Для выделения таких подсетей, из существующего адресного пространства, необходимо зарезервировать 2 старших бита (2^2 = 4 сети) из младшего байта IP-адреса.

192.168.1.0 /26 (255.255.255.192)

Получается 4 подсети, с адресами:

192.168.1.0 – 192.168.1.63(vlan1)

Адрес сети: 192.168.1.0

Адреса хостов:192.168.1.1 – 192.168.1.62

Широковещательный адрес: 192.168.1.63
192.168.1.64 – 192.168.1.127 (vlan2)
Адрес сети: 192.168.1.64
Адреса хостов:192.168.1.65 – 192.168.1.126
Широковещательный адрес:192.168.1.127

192.168.1.128 – 192.168.1.191 (vlan3)
Адрес сети: 192.168.1.128
Адреса хостов:192.168.1.129 – 192.168.1.190
Широковещательный адрес:192.168.1.191

192.168.1.192 – 192.168.1.255 (vlan4)
Адрес сети: 192.168.1.192
Адреса хостов:192.168.1.193 – 192.168.1.254
Широковещательный адрес:192.168.1.255

2. Анализ предметной области

Для проектирования корпоративной сети была выбрана организация «KEGOC».

2.1 Обследование предприятия и его информационные запросы

Акционерное общество «Казахстанская компания по управлению электрическими сетями» (АО «KEGOC»). Национальная электрическая корпоративная сеть обеспечивает транспортировку электроэнергии от энергопроизводителей, имеющих схему выдачи электроэнергии непосредственно в национальную корпоративная сеть до оптовых потребителей, подключенных к этой сети (распределительные электросетевые компании, крупные потребители). АО «KEGOC» поручены определение стратегии развития отрасли, формирование её технической политики, разработка перспективных планов и программ, ведение балансов. В корпорации постоянно проходит обмен данными, вследствие чего от компьютерно-коммуникационной системы требуется:

- доступ сотрудников компании к компьютерной сети Интернет;
- связь филиалов;
- сетевое хранение и публикация файлов и документов во внутренней сети.

Основными задачами проектируемой корпоративной сети являются:

- сетевое хранение файлов и сетевая печать;
- электронная почта и связь;
- коллективная работа и совместная обработка информации;
- высокопроизводительная система обмена информацией (База данных);
- централизованное управление компьютерами и обработки информации;
- контроль за доступом к важным данным;
- централизованное резервное копирование всех данных;
- публикация документов во внутренней сети и/или в Интернет (WWW сервер).

Руководство видит компанию как динамично расширяющуюся и развивающуюся организацию, поэтому основными требованиями, предъявляемыми к сетям являются следующие:

- она должна иметь достаточной производительностью;
- она должна легко управляемой, что позволяет без особых усилий подстраивать ее под меняющиеся потребности организации;
- корпоративная сеть должна масштабируемой, т.е. позволять легко увеличивать количество пользователей и используемых прикладных программ;

– корпоративная сеть должна иметь необходимой надежностью и безопасностью.

В данной организации уже развернута корпоративная сеть в масштабе нескольких городов республики. В дальнейшем возможно увеличение количества городов, в этой сети. В этом случае необходимо будет модернизировать существующую корпоративная сеть с применением более современного оборудования, программного обеспечения.

Решающими факторами при проектировании сети будут эффективная, безопасная работа системы с централизованным управлением базой данных, для чего корпоративная сеть должна построена на основе сервера.

Преимущества сети на основе сервера.

– разделение ресурсов. Сервер настроен так, чтобы предоставлять доступ к множеству файлов, обеспечивая при этом высокую производительность и защиту. Администрирование и управление данными осуществляется централизованно.

– защита. Проблемами безопасности может заниматься один администратор: он формирует политику безопасности и применяет ее в отношении каждого пользователя сети.

Резервное копирование данных. Поскольку жизненно-важная данные расположена централизованно, т.е. сосредоточена на серверах, нетрудно обеспечить ее регулярное резервное копирование.

– избыточность. Благодаря избыточным системам, данные на любом сервере могут дублироваться в определенном реальном времени, поэтому в случае повреждения основной области хранения данных данные не будет потеряна – легко воспользоваться резервной копией;

– количество пользователей. Сети на основе сервера способны поддерживать тысячи пользователей. Одноранговыми корпоративными сетями такого размера было бы невозможно управлять;

– аппаратное обеспечение. Так как компьютер не выполняет функций сервера, требования к его характеристикам зависят от определенных потребностей самого пользователя. [1]

2.2 Определение структуры потоков данных

Для проектирования сети нужно определить информационный поток предприятия, который должна обрабатывать проектируемая корпоративная сеть. Опираясь на то, что пользователями сети являются работники административно-управленческого персонала всего же трех подразделений, которые работают в свою очередь с узкоспециализированным программным обеспечением (1С Бухгалтерия, MSSQLServer т.д.) и количество рабочих станций (100), можно сделать вывод о том, что нагрузка на корпоративная сеть будет не особо значительной. Использование пользователь-серверной системы, также снижает информационный поток, поскольку здесь сервер применяется

только для предоставления доступа к приложениям и хранения сгенерированных данных. Вся обработка данных выполняется на рабочей станции, что улучшает производительность работы сети и снижает загруженность сервера.

Распределение компьютеров между уровеньями и филиалами:

Филиал №1 Астана (1 уровень). Количество рабочих станций - 20
Первый уровень (40 компьютеров).
Reception – 3 компьютер.
Технический отдел - 19 компьютера.
Разработчики – 18 компьютера.
Второй уровень (40 компьютеров).
Инженерный отдел 25 – компьютеров.
Отдел статистики и управления - 10 компьютеров.
Отдел кадров – 2 компьютера.
Юридический отдел – 2 компьютера.
Бухгалтерия – 1 компьютеров.

Филиал №2 Атырау (1 уровень). Количество рабочих станций - 20
Первый уровень (40 компьютеров).
Reception – 3 компьютер.
Юридический отдел – 7 компьютера.
Отдел кадров – 5 компьютера.
Бухгалтерия – 5 компьютеров.
Разработчики – 20 компьютера
Второй уровень (40 компьютеров).
Технический отдел - 40 компьютера.
Третий уровень уровень (40 компьютеров).
Инженерный отдел 30 – компьютеров
Отдел статистики и управления - 10 компьютеров.

3. Теоретические аспекты проектирования корпоративной сети

3.1 Протокол динамической конфигурации DHCP

DHCP (Dynamic Host Configuration Protocol -протокол динамической конфигурации) -это протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Для этого компьютер обращается к серверу, называемому сервером DHCP. Администратор может задать диапазон адресов, распределяемых среди компьютеров. Это позволяет избежать ручной настройки компьютеров и уменьшает количество ошибок. Протокол DHCP обычно применяется в большинстве крупных сетях TCP/IP.

Протокол DHCP предоставляет три способа распределения IP-адресов:

- Ручное распределение. При этом способе сетевой администратор сопоставляет определенному аппаратному адресу (обычно MAC-адресу) каждого такого пользовательского компьютера определённый IP-адрес. Данный способ распределения адресов отличается от ручной настройки каждого компьютера лишь тем, что сведения о таких адресах хранятся централизованно (на сервере DHCP), и потому их проще изменять и редактировать при необходимости.
- Автоматическое распределение. При данном способе каждому компьютеру на постоянное использование выделяется свободный и неповторяющийся IP-адрес из определённого администратором диапазона.
- Динамическое распределение. Этот способ аналогичен автоматическому распределению, за исключением того, что адрес выдаётся компьютеру не на постоянное пользование, а на определённый срок. Это называется арендой адреса. По истечении срока такой аренды IP-адрес вновь считается свободным, и пользователь корпоративной сети обязан запросить новый (он, впрочем, может оказаться тем же самым).

Некоторые службы DHCP способны автоматически обновлять данные определенные DNS, относящихся к пользовательским компьютерам, при определении им новых адресов. Это производится определенно при помощи протокола обновления DNS.

Нахождение DHCP

Сначала пользователь выполняет широковещательный запрос по всей корпоративной сети с целью найти доступные DHCP-серверы. Он посылает сообщение вида DHCPDISCOVER, при этом в качестве IP-адреса указывается 0.0.0.0 (так как компьютер ещё не имеет собственного IP-адреса), а в качестве адреса назначения -широковещательный адрес 255.255.255.255.

Пользователь заполняет несколько полей сообщения начальными значениями:

- В поле xid помещается уникальный идентификатор транзакции, который помогает отличать данный процесс получения IP-адреса от других,

протекающих в то же время.

– В поле chaddr помещается аппаратный адрес (MAC-адрес) пользователя.

– В поле опций указывается предыдущий известный пользователю IP-адрес. В данном примере - 192.168.1.100. Это необязательно и может проигнорировано сервером.

Сообщение DHCPDISCOVER может распространено за пределы локальной физической сети благодаря специально настроенным агентам ретрансляции DHCP, перенаправляющих поступающие от пользователей данные DHCP серверам в других подсетях.

Предложение *DHCP*

Получив сообщение от определенного пользователя, сервер находит требуемую конфигурацию пользователя в соответствии с указанными сетевым администратором настройками. В данном случае DHCP-сервер согласен с запрошенным пользователем адресом 192.168.1.100. Сервер посылает ему ответ (DHCPOFFER), в котором определяет конфигурацию. Предлагаемый пользователю IP-адрес указывается в поле. Прочие параметры (такие, как адреса маршрутизаторов и DNS-серверов) указываются в виде опций в соответствующем поле.

Это сообщение DHCP-сервер посылает хосту пославшему (DHCPDISCOVER) на его MAC, при определенных обстоятельствах таким обраоз может распространяться, как широковещательная определенная рассылка. Пользователь может получить множество различных и вариативных предложений DHCP от разных серверов; из них он должен выбрать то, которое его «удовлетворяет».

Запрос DHCP

Определив одну из конфигураций, предложенных DHCP-серверами, пользователь посылает запрос DHCP (DHCPREQUEST). Он рассылается широковещательно; при этом к опциям, указанным пользователем в сообщении DHCPDISCOVER, добавляется специальная опция -идентификатор сервера - указывающая адрес DHCP-сервера, выбранного пользователем (в данном случае - 192.168.1.1).

Подтверждение DHCP

Наконец, сервер подтверждает запрос и направляет это подтверждение (DHCPACK) пользователю. После этого пользователь должен настроить свой сетевой интерфейс, используя предоставленные опции.

Отказ DHCP

Если после получения сигнала (DHCPACK) от сервера пользователь обнаруживает, что указанный сервером адрес уже применяется в сети, он рассылает широковещательное сообщение отказа DHCP (DHCPDECLINE), после чего процедура получения этих IP-адреса повторяется. Использование IP-адреса другим пользователем можно обнаружить, выполнив запрос ARP.

Отмена DHCP

Если по каким-то причинам сервер не может предоставить пользователю

запрошенный IP-адрес, или аренда адреса убирается администратором, сервер расспределяет широковещательное сообщение отмены DHCP (DHCPNAK). При получении этого сообщения соответствующий пользователь обязан повторить процедуру получения адреса.

Освобождение DHCP

Пользователь легко может открытым образом прекратить аренду IP-адреса. Для этого он посылает сообщение DHCP (DHCPRELEASE) тому серверу, который предоставил ему адрес в аренду. В отличие от других сообщений DHCP, DHCPRELEASE не рассылается широковещательно.

3.2 DNS

DNS (англ. Domain Name System -система доменных имён) – система, способная по запросу, содержащему доменное имя, сообщить IP адрес другую информацию. DNS работает в сетях TCP/IP. DNS может хранить и обрабатывать и обратные запросы, определения имени хоста по его IP адресу - IP адрес по правилу преобразуется в доменное имя, и посылается запрос на информацию типа "PTR".

DNS имеет следующими характеристиками:

- Распределённость хранения данных. Каждый участок сети в обязательном порядке должен хранить только те данные, которые входят в его сферу ответственности и адреса корневых DNS-серверов.
- Кеширование информации. Участок может хранить в себе некоторое количество определенных данных не из своей зоны ответственности для уменьшения нагрузки на остальную корпоративная сеть.
- Резервирование. За хранение и обслуживание своих узлов (зон) отвечают несколько серверов, распределённые выполняются как физически, так и логически, что обеспечивает сохранность данных и продолжение работы даже в случае сбоя одного из узлов.

Структура такого взаимодействия с серверами имен представлен на рисунке 3.2.1. Пример формата DNS-сообщений представлен на рисунке 3.2.2.

Каждое такое сообщение начинается с заголовка, который содержит в себе поле идентификация, позволяющее связать в пару запрос и отклик. Поле флаги определяет свойства запрашиваемой процедуры, а также кодировку отклика. Поля число определяют количество потому и были определенных записей соответствующего типа, содержащихся в сообщении. Так число запросов задает число записей в секции запросов, где записаны запросы, требующие ответов.

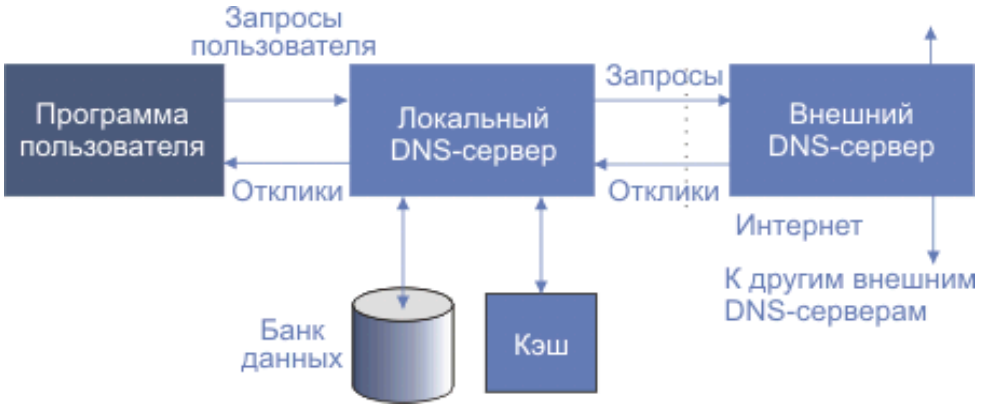

Рисунок 3.2.1 - Структура взаимодействия с серверами имен

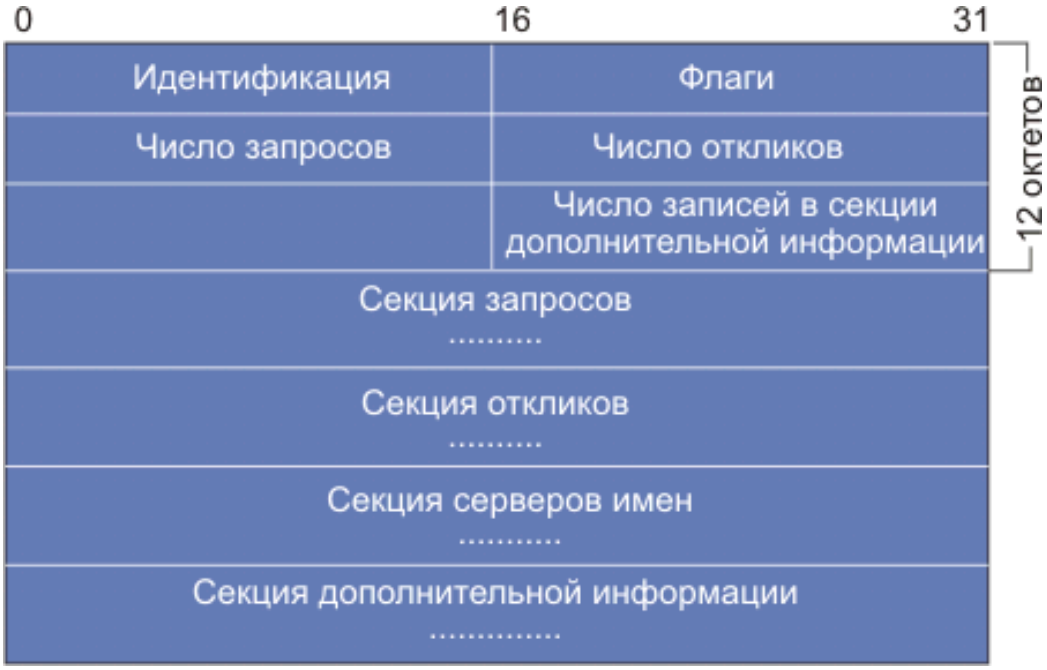

Рисунок 3.2.2 - Формат DNS-сообщений

Каждый вопрос состоит из символьного имени домена, за которым следует тип запроса и класс запроса.

Значения битов поля в сообщении сервера имен отображены в таблице 3.2. Разряды пронумерованы слева направо, начиная с нуля рис. 3.2.3.

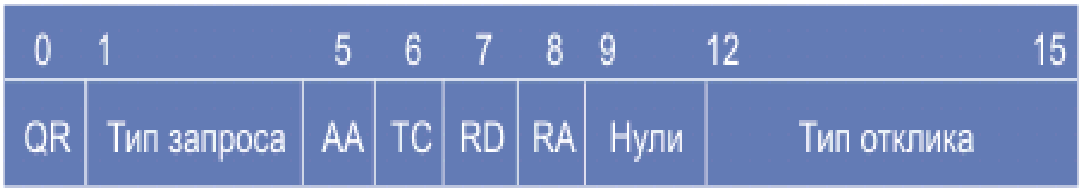

Рисунок 3.2.3 - Назначение битов поля флаги.

Таблица 3.2 Коды поля флаги

Код поля флаги	Описание	
0 (QR)	Операция:	0 Запрос 1 Отклик
1…4	Тип запроса (opcode):	0 стандартный 1 инверсный 2 запрос состояния сервера
5 (AA)	Равен 1 при отклике от сервера (RR), в ведении которого находится домен, упомянутый в запросе.	
6 (TC)	Равен 1 при укорочении сообщения. Для UDP это означает, что ответ содержал более 512 октетов, но прислано только первые 512.	
7 (RD)	Равен 1, если для получения ответа желательна рекурсия.	
8 (RA)	Равен 1, если рекурсия для запрашиваемого сервера доступна.	
9…11	Зарезервировано на будущее. Должны равняться нулю.	
12…15	Тип отклика (rcode):	0 нет ошибки 1 ошибка в формате запроса 2 сбой в сервере 3 имени не существует

3.3 HTTP-сервер

Веб-сервер -это сервер, принимающий HTTP-запросы от пользователей, обычно веб-браузеров, и выдающий им HTTP-ответы, обычно вместе с HTML-страницей, изображением, файлом, медиа-потоком или другими данными.

Веб-сервером называют как ПО, выполняющее определенные возможные функции веб-сервера, так и компьютер, на котором это программное обеспечение работает.

Пользователи получают определенный доступ к веб-серверу по URL адресу нужной им веб-страницы или другого ресурса.

Дополнительные возможности

Дополнительными возможностями многих веб-серверов являются:

- ведение журнала записи пользователей к ресурсам;
- аутентификация большого количества пользователей;
- поддержка нескольких динамически генерируемых страниц;
- поддержка HTTPS для защищённых компьютерных соединений с пользователями.

Пользователь

В качестве пользователя для обращения к таким веб-серверам могут использоваться совершенно различные устройства:

- Веб-браузер - самый распространенный и простой способ.
- Специальное программное обеспечение может самостоятельно

обращаться к веб-серверам для получения обновлений или другой информации.

- Мобильный телефон может получить доступ к ресурсам веб-сервера при помощи определенного протокола.
- Другие устройства или бытовая техника.

3.4 Протокол RIP

Протокол RIP (Routing Information Protocol) -протокол маршрутизации, который дает возможность маршрутизаторам динамически обновлять маршрутные данные, получая ее от соседних роутеров.

RIP - дистанционно-векторный протокол, который работает оперируя хопами в качестве метрики маршрутизации. Количество использованных хопов, разрешенное в RIP -15 (метрика 16 означает «бесконечную метрику»). Каждый RIP-маршрутизатор по умолчанию вещает а также в корпоративная сеть свою полную таблицу маршрутизации раз в 25 секунд, генерируя довольно много необходимого трафика на низкоскоростных линиях связи. RIP работает на прикладном уровне стека TCP/IP, используя UDP порт 521.

Рисунок 3.4 - Формат сообщений протокола RIP-2

Протокол RIP-2 является новой, обновленной версией RIP, которая в дополнение к широковещательному режиму поддерживает так же и мульти-кастинг; позволяет работать с большими масками суб-сетей. На рисунке 3.4 представлен вид сообщения для протокола RIP-2. Поле маршрутный демон является идентификатором программы-маршрутизатора. Поле метка маршрута применяется для поддержки необходимых внешних протоколов маршрутизации, сюда записываются коды автономных систем. При

необходимости управления доступом можно использовать первые 20 байт с кодом набора протоколов сети 0xFFFF и меткой маршрута =2. Тогда в остальные 16 байт можно записать пароль.

3.5 Протокол OSPF

OSPF (Open Shortest Path First) -протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути Алгоритм Дейкстры (Dijkstra's algorithm).

OSPF предлагает решение следующих задач:

- Увеличение скорости сходимости;
- Поддержка сетевых масок переменной длины (VLSM);
- Достижимость корпоративной сети (мгновенно обнаруживаются отказавшие маршрутизаторы, и топология сети изменяется соответствующим образом);
- Оптимальное использование пропускной способности (т.к строится минимальный остовный граф по алгоритму Дейкстры);
- Метод выбора пути.

Рисунок 3.5 Формат заголовка сообщений для протокола маршрутизации ospf

Описание работы протокола

1) Маршрутизаторы обмениваются hello-пакетами через все интерфейсы, на которых настроен OSPF. Маршрутизаторы, разделяющие общий канал передачи данных, становятся соседями, когда они приходят к договоренности об определенных параметрах, указанных в их hello-пакетах.

2) На следующем этапе работы протокола маршрутизаторы будут пытаться переключится в состояние соседства с маршрутизаторами, находящимися с ним в пределах прямой связи .Переход в состояние соседства определяется типом маршрутизаторов, обменивающихся hello-пакетами, и типом сети, по которой таки образом передаются hello-пакеты. OSPF определяет несколько типов сетей и несколько типов маршрутизаторов. Пара

маршрутизаторов, находящихся в состоянии соседства, синхронизирует между собой базу данных состояния каналов.

3) Каждый роутер посылает объявление о состоянии канала маршрутизаторам, с которыми он находится в состоянии соседства.

4) Каждый роутер, получивший объявление от соседа, записывает передаваемую в нём информацию в базу данных состояния такого каналов маршрутизатора и рассылает копию объявления всем другим своим определенным соседям.

5) Рассылая определенные сообщения через зону, все роутеры вместо строят идентичную базу данных состояния каналов маршрутизатора.

6) Когда база данных построена, каждый маршрутизатор использует алгоритм «кратчайший путь первым» определенных для вычисления графа без петель, который будет описывать кратчайший путь к каждому известному пункту назначения с собой в качестве корня. Этот граф -это дерево кратчайшего пути.

7) Каждый роутер строит таблицу маршрутизации из своего дерева кратчайшего пути.

3.6 Построение VLAN

VLAN (Virtual Local Area Network) -виртуальная локальная вычислительная корпоративная сеть, подразумевает группу хостов с общим набором правил, которые взаимодействуют потому что так, как если бы они были подключены к широковещательному определенному домену, независимо от их физического местонахождения. VLAN обладает теми же свойствами, что и физическая локальная корпоративная сеть, но позволяет конечным станциям, группироваться вместе, даже если они таких и не находятся определенно в одной физической сети. Такая реорганизация может сделана на основе программного обеспечения вместо физического перемещения устройств.

Регламентирующий стандарт: IEEE 802.1

Стандарт IEEE 802.1 показывает один протокольный блок данных (PDU), который носит название SDE (Secure Data Exchange) PDU. Заголовок пакета IEEE 802.1 имеет внутреннюю и внешнюю секции и показан на рисунке 3.6.

Рисунок 3.6 Формат пакета IEEE 802.1

Новый заголовок включает в себя три субполя. MDF (Management Defined

Field) содержит информацию о способе обработки PDU. Четырехбайтовое субполе SAID (Security Association Identifier) - идентификатор сетевого объекта (VLAN ID). Субполе 802.1 LSAP (Link Service Access Point) представляет собой код, указывающий принадлежность пакета к протоколу vlan. Предусматривается режим, когда применяется определенно только этот заголовок.

Безопасный заголовок копирует себе адрес отправителя из mac-заголовка (MAC - Media Access Control), что повышает надежность.

Поле ICV (Integrity Check Value) - служит для защиты пакета от незапланированной такой модификации. Для настроек VLAN используется защищенная управляющая база данных SMIB(security management information base).

Наличие VLAN ID (SAID) в пакете определяет его из общего потока и переправляет на опорную магистраль, через которую и осуществляется доставка нужному адресату. Размер поля DATA определяется физической сетевой средой.

3.7 Маршрутизация VLAN

Для переключения трафика принадлежащего нескольким VLAN между коммутаторами по одному и тому же линку используются магистральные каналы или транки. Оборудование может найти к какому VLAN принадлежит трафик по его идентификатору VLAN. Идентификатор VLAN - это обозначение, которая инкапсулируется в данные. Для переноса данных от нескольких VLAN по каналам используются три типа инкапсуляции ISL и 802.1Q

ISL – это протокол разработанный компанией Cisco для соединения свитчей друг с другом и поддержания данных о VLAN в трафике, проходящем через них. ISL использует группообразование VLAN в единый магистральный канал на поной скорости соединения Ethernet в полнодуплексном или полудуплексном режиме. ISL работает в среде точка-точка и может поддерживать вплоть до 1000 VLAN. При ISL инкапсуляции к оригинальному фрейму добавляется заголовок ISL, оригинальный пакет остается в неизменном виде, а также в конце фрейма имеет и добавляется новая контрольная сумма - FCS (Frame Check Sequence). Контрольная сумма оригинального пакета остается БЕЗ изменений. Затем полученный кадр передается в магистральный канал. На приемной стороне, заголовок ISL удаляется и кадр пересылается в назначенный VLAN.

802.1Q это стандарт IEEE. IEEE 802.1Q использует внутренний механизм тагирования, который добавляет к оригинальному фрейму 4 байта, вставляя тэг между MAC-адресом источником и полем Type/Length фрэйма Ethernet. После добавления тега пересчитывается контрольная сумма оригинального фрейма.

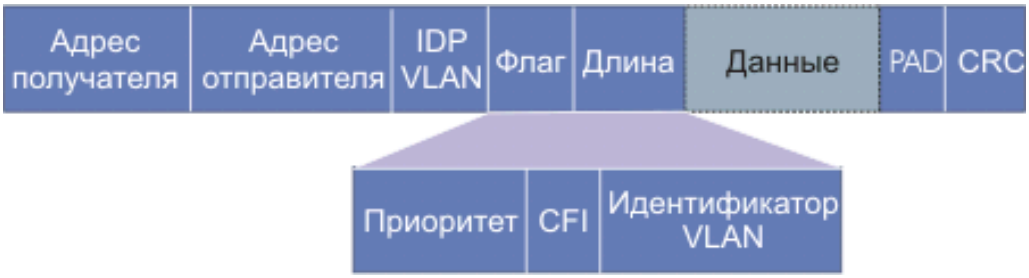

Рисунок 3.7 Формат кадра 802.1Q.

Структура полей флаг и длина представлена в нижней части рисунка. Поле идентификатор VLAN имеет длину 12 бит определяет, какой виртуальной сети принадлежит кадр. Поле приоритет (три бита) позволяет выделять трафик реального времени, трафик со средними такими требованиями и трафик, для которого время доставки не критично. Это открывает возможность использования Ethernet для задач управления и обеспечения огромного качества обслуживания при транспортировке мультимедийных данных. Однобитовое поле CFI (Canonical Format Indicator) первоначально определял, прямой или обратный порядок байт применяется. В настоящее время его функцией (=1) является указание того, что в поле данных содержится кадр 802.5 Размер Фрэйма

Протокол 802.1Q использует вставку (тег) в оригинальный заголовок фрейма, длинной 4 байта, таким образом максимальный размер фрейма может 1522 байта, т.е. 1518 байт для Ethernet пакета плюс 4 байта заголовка. Минимальный размер самого большого тегированного фрейма может составлять 68 байт для технологии Ethernet. Стоит отметить, что при работе по протоколу 802.1Q изменяется непосредственно оригинальный фрейм - вставляется дополнительное поле и пересчитывается контрольная сумма - FCS. Формат 802.1Q-тега несколько проще, чем при инкапсуляции ISL, однако есть и свои преимущества:

- размер тегированного фрейма меньше;
- максимальное количество возможных VLAN-ов увеличено в 4 раза (4095).

3.8 Протокол NAT

NAT (от англ. Network Address Translation -«преобразование сетевых адресов») -это система в сетях TCP/IP, позволяющий преобразовывать IP-адреса пакетов.

Преобразование адресов с использование NAT может производиться почти любым маршрутизирующим устройством -маршрутизатором, сервером доступа, сетевым экраном. Сысл механизма состоит в замене адреса источника (source) при прохождении пакета в одну сторону и замене такого адреса назначения (destination) в ответном пакете. Наряду с source/destination могут

также заменяться нумерация портов source/destination.

Помимо source NAT (предоставления участникам локальной сети с внутренними адресами доступа к сети Интернет) часто используют также destination NAT, когда обращения снаружи понятие определенно транслируются межсетевым экраном на сервер в локальной сети, имеющий внутренний адрес и потому недоступный извне сети непосредственно (без NAT).

Существует 3 базовых концепции трансляции адресов: статическая (Static Network Address Translation), динамическая (Dynamic Address Translation), маскарадная (NAPT, PAT).

Механизм NAT определён в RFC 1631, RFC 3022.

Преимущества

NAT выполняет две важные функции.

1. Возможность сэкономить IP-адреса, транслируя несколько внутренних IP-адресов в один внешний публичный IP-адрес (или в несколько, но меньшим количеством, чем внутренних).

2. Возможность предотвратить или ограничить обращение снаружи к хостам, оставляя возможность обращения изнутри наружу. При определении соединения изнутри сети создаётся трансляция. Пакеты, поступающие снаружи, соответствуют созданной трансляции о том и поэтому пропускаются. Если для пакетов, поступающих снаружи, соответствующей той трансляции не существует (а она может созданной при инициации соединения или статической), они не пропускаются.

Минусы

1. Не все протоколы могут «пройти» NAT. Некоторые не в состоянии работать, если на пути между взаимодействующими хостами есть трансляция адресов. Некоторые межсетевые экраны, выполняющие трансляцию IP-адресов, могут исправить этот недостаток, соответствующим образом заменяя IP-адреса не только в заголовках IP, но и на более высоких уровнях (например, в командах протокола FTP). См. Application-level gateway.

2. Из-за трансляции адресов «много в один» появляются дополнительные сложности с идентификацией пользователей и необходимость хранить полные логи трансляций.

3. DoS со стороны узла, осуществляющего NAT -если NAT применяется для подключения многих пользователей к одному и тому же службау, это может вызвать иллюзию DoS атаки на служба (множество успешных и неуспешных попыток). Например, избыточное количество таких пользователей ICQ за NAT’ом приводит к проблеме подключения таких некоторых пользователей из-за превышения допустимой скорости коннектов к серверу. Частичным решением такой проблемы является ограниченное использование пула адресов (группы адресов), для которых осуществляется трансляция.

4. Сложности в работе с пиринговыми сетями, в которых необходимо не только инициировать исходящие соединения, но также принимать входящие.

4. Применение настроек конфигурации сети

Проанализировав проектируемое рабочее место (рисунок 4.1), была спроектирована тополгия сети, представленная на рисунке 4.2.

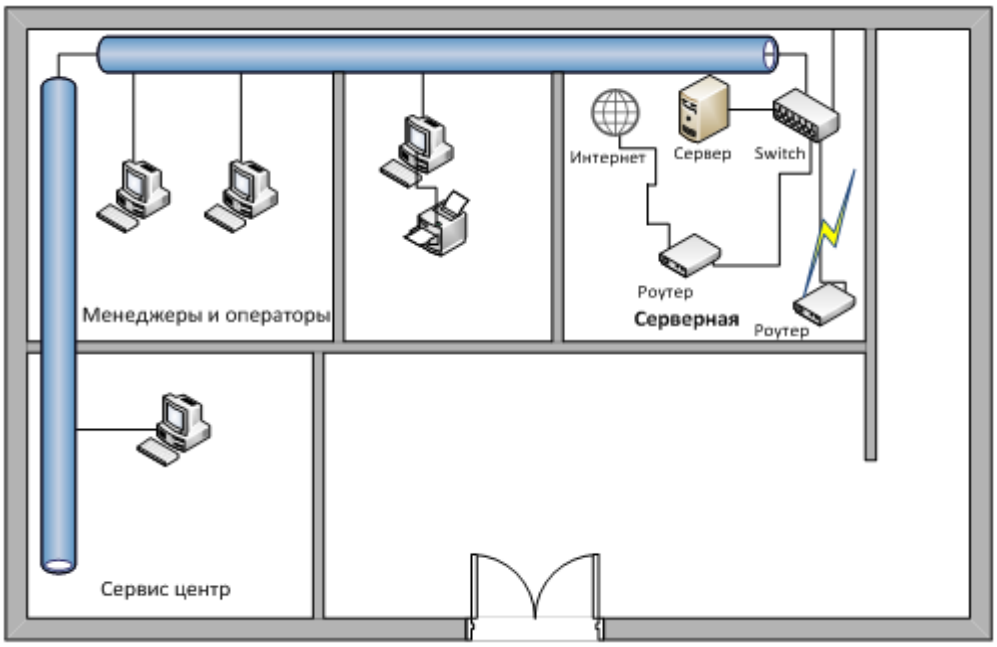

Рисунок 4.1 – Проектируемое рабочее место

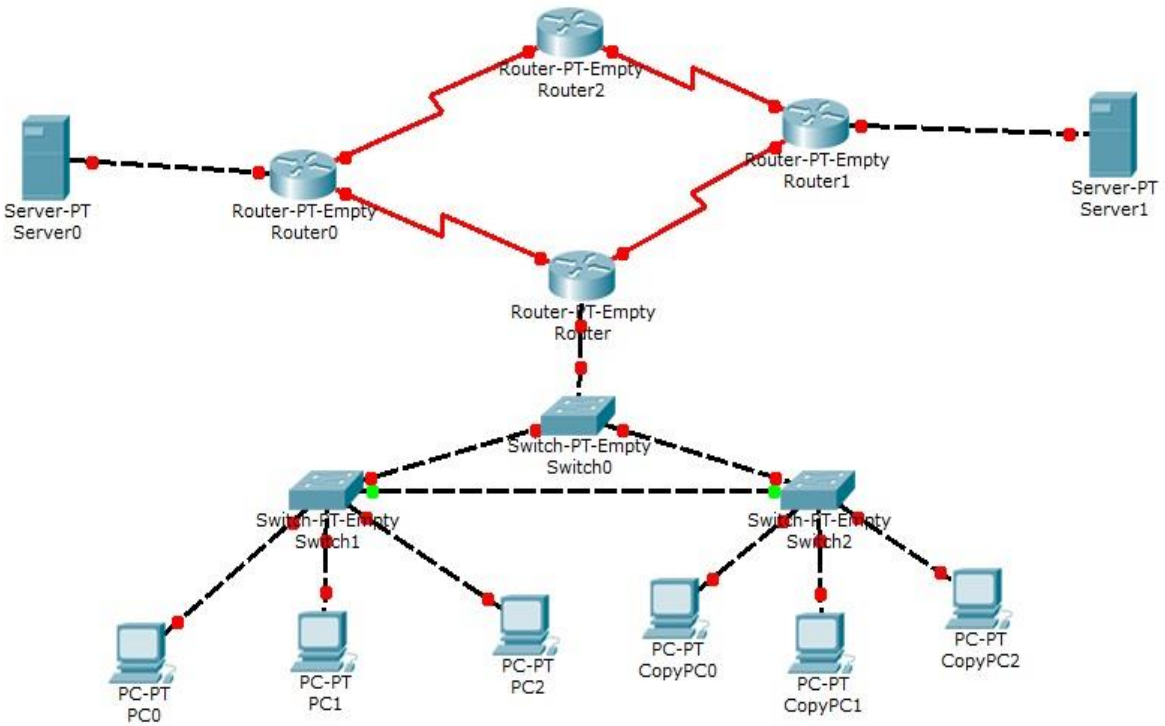

Рисунок 4.2 – Топология сети до настроек

Далее производятся настройки сети для дальнейшей возможности передачи сообщений.

Настройка DHCP

На каждом маршрутизаторе прописываем интерфейсы соответственно заданию:

```
Router(config)# ip dhcp pool 1
Router(config)# network 192.168.1.0 255.255.255.192
Router(config)# default-router 192.168.1.1
Router(config)# dns-server 15.12.2.2

Router(config)# ip dhcp pool 2
Router(config)# network 192.168.1.64 255.255.255.192
Router(config)# default-router 192.168.1.65
Router(config)# dns-server 15.12.2.2

Router(config)# ip dhcp pool 3
Router(config)# network 192.168.1.128 255.255.255.192
Router(config)# default-router 192.168.1.129
Router(config)# dns-server 15.12.2.2

Router(config)# ip dhcp pool 4
Router(config)# network 192.168.1.192 255.255.255.192
Router(config)# default-router 192.168.1.193
Router(config)# dns-server 15.12.2.2
```

Настройка DNS

В настройках DNS сервера указываем IP-адрес самого сервера с маской (15.15.2.2 255.255.255.0) и IP-адрес шлюза по умолчанию (15.15.2.1).Так же указываем доменное имя и IP-адрес HTTP-сервера (15.15.5.2).

Настройка HTTP-сервера

В параметрах HTTP-сервера настраиваем IP-адрес самого сервера с маской подсети (15.15.5.2 255.255.255.0). Так же можем выполнить ввод базовой страницы определенного сервера, которая будет выводиться на запрос браузера после обращения по доменному имени, которому в следствии приравнен IP адрес этого HTTP-сервера. Для этого нужно выполнить настройки HTTP-сервера и DNS-сервера.

Настройка DNS-сервера показана на рисунках 4.3 и 4.4.

Настройка протокола RIP

На маршрутизаторах нашей сети пропишем действия протокола RIP.

```
Router(config)# router rip
Router(config-router)# network 192.168.1.0
```

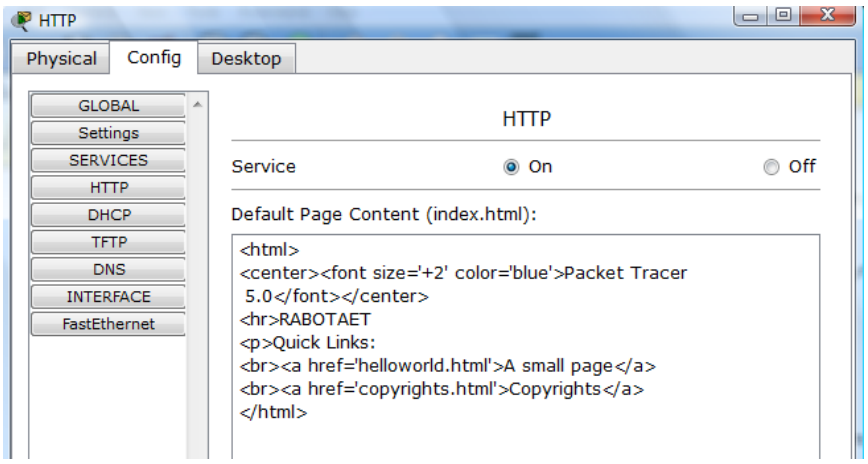

Рисунок 4.3 Настройка DNS-сервера.

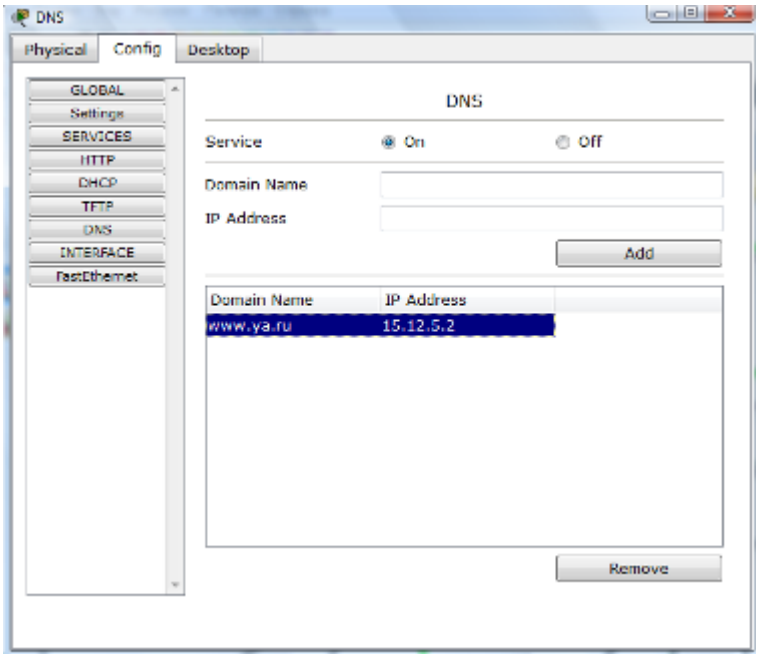

Рисунок 4.2 Настройка DNS-сервера.

```
Router(config-router)# network 15.15.1.0
Router(config-router)# network 15.15.6.0
Router(config)# router rip
Router(config-router)# network 15.15.1.0
Router(config-router)# network 15.15.2.0
Router(config-router)# network 15.15.3.0

Router(config)# router rip
Router(config-router)# network 15.15.3.0
Router(config-router)# network 15.15.4.0

Router(config)# router rip
Router(config-router)# network 15.15.4.0
Router(config-router)# network 15.15.5.0
```

Настройка OSPF

На соответствующих маршрутизаторах нашей сети пропишем действия протокола OSPF.

```
Router(config)# router ospf 100
Router(config-router)# network 192.168.1.0 0.0.0.63 area 0
Router(config-router)# network 192.168.1.64 0.0.0.63 area 0
Router(config-router)# network 192.168.1.128 0.0.0.63 area 0
Router(config-router)# network 192.168.1.192 0.0.0.63 area 0
Router(config-router)# network 15.15.1.0 0.0.0.255 area 0
Router(config-router)# network 15.15.6.0 0.0.0.255 area 0

Router(config)# router ospf 100
Router(config-router)# network 15.15.1.0 0.0.0.255 area 0
Router(config-router)# network 15.15.2.0 0.0.0.255 area 0
Router(config-router)# network 15.15.3.0 0.0.0.255 area 0

Router(config)# router ospf 100
Router(config-router)# network 15.15.3.0 0.0.0.255 area 0
Router(config-router)# network 15.15.4.0 0.0.0.255 area 0

Router(config)# router ospf 100
Router(config-router)# network 15.15.4.0 0.0.0.255 area 0
Router(config-router)# network 15.15.5.0 0.0.0.255 area 0
Router(config-router)# network 15.15.6.0 0.0.0.255 area 0
```

Настройка VLAN

Перед тем, как начать настройку VLAN, нужно сначала произвести настройки определенных устраивающих рабочих станций. В разделе IP configuration удостоверится, что стоит динамическая раздача адресов(.

Пропишем vlan-ы на каждом коммутаторе

Vlan 1 на коммутаторах можно не прописывать, так как она существует по умолчанию.

Для конфигурирования коммутаторов нужно перейти в CLI-режим коммутатора.

```
Switch 1
Switch> enable  //Вход в привилегированный режим
Switch# configure terminal //Вход в режим глобальной конфигурации
Switch(config)# vlan 2 //Прописывание vlan 2
Switch(config-vlan)# name vlan_2 //Назначение имени «vlan_2»
Switch(config-vlan)# exit//Выход из режима конфигурации vlan 2
Switch(config)# vlan 3 //Прописывание vlan 3
Switch(config-vlan)# name vlan_3//Назначение имени «vlan_3»
Switch(config-vlan)# exit//Выход из режима конфигурации vlan 3
Switch(config)# exit //Выход из режима глобальной конфигурации
 Switch#show vlan //Проверка таблицы vlan-ов
```

```
Switch 2
Switch> enable Вход в привилегированный режим
Switch# configure terminalВход в режим глобальной конфигурации
Switch(config)# vlan 4Прописывание vlan 4
Switch(config-vlan)# name vlan_4Назначение имени «vlan_4»
Switch(config-vlan)# exitВыход из режима конфигурации vlan 4
Switch(config)# vlan 3Прописывание vlan 3
Switch(config-vlan)# name vlan_3Назначение имени «vlan_3»
Switch(config-vlan)# exitВыход из режима конфигурации vlan 3
Switch(config)# exitВыход из режима глобальной конфигурации
Switch#show vlanПроверка таблицы vlan-ов

Switch 3
Switch> enable Вход в привилегированный режим
Switch# configure terminalВход в режим глобальной конфигурации
Switch(config)# vlan 4Прописывание vlan 4
Switch(config-vlan)# name vlan_4Назначение имени «vlan_4»
Switch(config-vlan)# exitВыход из режима конфигурации vlan 4
Switch(config)# vlan 2Прописывание vlan 2
Switch(config-vlan)# name vlan_2Назначение имени «vlan_2»
Switch(config-vlan)# exitВыход из режима конфигурации vlan 2
Switch(config)# exitВыход из режима глобальной конфигурации
Switch#show vlanПроверка таблицы vlan-ов

Switch 4
Switch> enable Вход в привилегированный режим
Switch# configure terminalВход в режим глобальной конфигурации
Switch(config)# vlan 2Прописывание vlan 2
Switch(config-vlan)# name vlan_2Назначение имени «vlan_2»
Switch(config-vlan)# exitВыход из режима конфигурации vlan 2
Switch(config)# vlan 3Прописывание vlan 3
Switch(config-vlan)# name vlan_3Назначение имени «vlan_3»
Switch(config-vlan)# exitВыход из режима конфигурации vlan 3
Switch(config)# vlan 4Прописывание vlan 4
Switch(config-vlan)# name vlan_4Назначение имени «vlan_4»
Switch(config-vlan)# exitВыход из режима конфигурации vlan 4
Switch(config)# exitВыход из режима глобальной конфигурации
Switch#show vlanПроверка таблицы vlan-ов
```

На свитчах уровня доступа, соотнесем порты к соответствующим vlan-м.

По умолчанию портам соответствует vlan 1. Поэтому назначения соответствующего порта можно пропустить.

```
Switch 1
Switch> enable Вход в привилегированный режим
Switch# configure terminalВход в режим глобальной конфигурации
Switch(config)# interface fa 0/2Вход в режим конфигурации интерфейса fa 0/2
Switch(config-if)# switchport access vlan 2 Назначаем порту
```

```
доступа vlan 2
     Switch(config-if)#   exitВыходим   из   режима   конфигурации
интерфейса
     Switch(config)#  interface  fa  0/3Вход  в  режим  конфигурации
интерфейса fa 0/3
     Switch(config-if)# switchport access vlan 3 Назначаем порту
доступа vlan 3
     Switch(config-if)#   exitВыходим   из   режима   конфигурации
интерфейса
     Switch(config)# exitВыход из режима глобальной конфигурации
     Switch#show vlanПроверка таблицы vlan-ов

     Switch 2
     Switch> enable Вход в привилегированный режим
     Switch# configure terminalВход в режим глобальной конфигурации
     Switch(config)#  interface  fa  0/1Вход  в  режим  конфигурации
интерфейса fa 0/1
     Switch(config-if)# switchport access vlan 4 Назначаем порту
доступа vlan 4
     Switch(config-if)#   exitВыходим   из   режима   конфигурации
интерфейса
     Switch(config)#  interface  fa  0/3Вход  в  режим  конфигурации
интерфейса fa 0/3
     Switch(config-if)# switchport access vlan 3 Назначаем порту
доступа vlan 3
     Switch(config-if)#   exitВыходим   из   режима   конфигурации
интерфейса
     Switch(config)# exitВыход из режима глобальной конфигурации
     Switch#show vlanПроверка таблицы vlan-ов

     Switch 3
     Switch> enable Вход в привилегированный режим
     Switch# configure terminalВход в режим глобальной конфигурации
     Switch(config)#  interface  fa  0/1Вход  в  режим  конфигурации
интерфейса fa 0/1
     Switch(config-if)# switchport access vlan 4 Назначаем порту
доступа vlan 4
     Switch(config-if)#   exitВыходим   из   режима   конфигурации
интерфейса
     Switch(config)#  interface  fa  0/2Вход  в  режим  конфигурации
интерфейса fa 0/2
     Switch(config-if)# switchport access vlan 2 Назначаем порту
доступа vlan 2
     Switch(config-if)#   exitВыходим   из   режима   конфигурации
интерфейса
     Switch(config)# exitВыход из режима глобальной конфигурации
     Switch#show vlanПроверка таблицы vlan-ов
```

Прописывание транковые портов на коммутаторах.

```
     Switch 1
```

```
Switch> enable Вход в привилегированный режим
Switch# configure terminalВход в режим глобальной конфигурации

Switch(config)# interface gi 1/1Вход в режим конфигурации
интерфейса gi 1/1
Switch(config-if)# switchport mode trunk Перевод порт в
транковый режим
Switch(config-if)# exitВыход из режима конфигурации интерфейса
```

Аналогично прописать транковые порты на Switch 2 и Switch 3.

```
Switch 4
Switch> enable Вход в привилегированный режим
Switch# configure terminalВход в режим глобальной конфигурации

Switch(config)# interface gi 9/1Вход в режим конфигурации
интерфейса gi 9/1
Switch(config-if)# switchport mode trunk Перевод порт в
транковый режим
Switch(config-if)# exitВыход из режима конфигурации интерфейса
```

Настройка маршрутизации VLAN

Создаем подинтерфейсы на маршрутизаторе

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet9/0
Router(config-if)# no shutdown
Router(config)# interface GigabitEthernet9/0.1
Router(config-subif)# encapsulation dot1Q 1
Router(config-subif)# ip address 192.168.1.1 255.255.255.192
Router(config-subif)# exit
Router(config)# interface GigabitEthernet9/0.2
Router(config-subif)# encapsulation dot1Q 2
Router(config-subif)# ip address 192.168.1.65 255.255.255.192
Router(config-subif)# exit
Router(config)# interface GigabitEthernet9/0.3
Router(config-subif)# encapsulation dot1Q 3
Router(config-subif)# ip address 192.168.1.129 255.255.255.192
Router(config-subif)# exit
Router(config)# interface GigabitEthernet9/0.4
Router(config-subif)# encapsulation dot1Q 4
Router(config-subif)# ip address 192.168.1.193 255.255.255.192
Router(config-subif)# exit
```

Настройка проткола STP

На корневом коммутаторе пропишем конфигурацию протокола STP

```
Switch(config)# spanning-tree vlan 1 root primary
Switch(config)# spanning-tree vlan 2 root primary
Switch(config)# spanning-tree vlan 3 root primary
Switch(config)# spanning-tree vlan 4 root primary
```

Настройка протокола NAT

Прописываем настройки протокола NAT на первом маршрутизаторе (router 1).

```
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip nat inside

Router(config)# interface FastEthernet1/0
Router(config-if)# ip nat outside

Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# ip nat pool work 15.15.1.1 15.15.1.15 netmask
255.255.255.0
Router(config)# ip nat inside source list 1 pool work
```

Топология настроенной сети представлена на рисунке 4.3

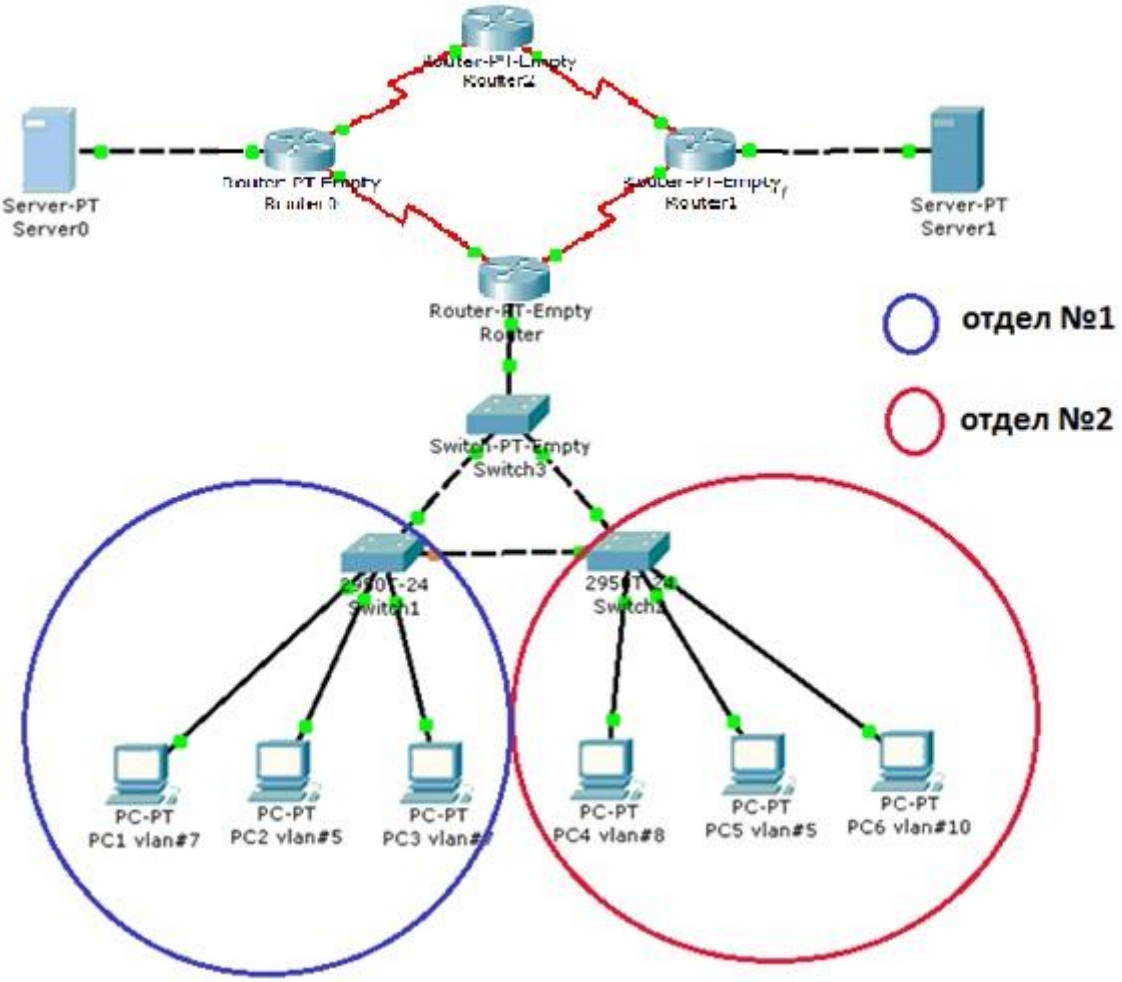

Рисунок 4.3 – Тополгия сети после настроек

5. Тестирование сети

Для тестирования сети отправим эхо – запросы.

Эхо запрос с 131.31.0.1 на 210.10.10.1, показан на рисунке 5.1.

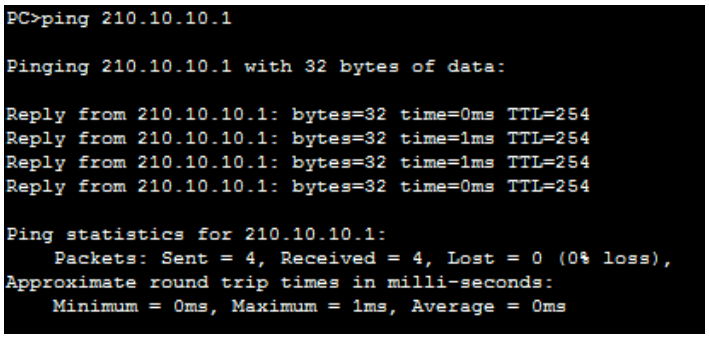

Рисунок 5.1 – Выход в интернет сотрудников Головного офиса

Эхо запрос с 131.31.0.5 на 131.31.128.4, показан на рисунке 5.2.

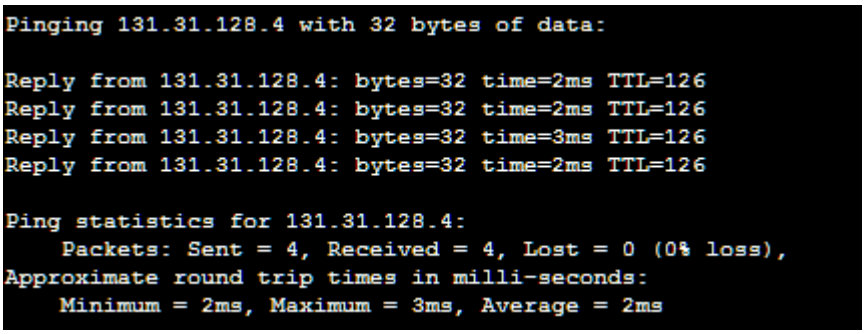

Рисунок 5.2 – Доступ к серверу из Головного офиса в Филиал Атырау

6. Планирование информационной безопасности

Защита данных включает в себя набор мероприятий, направленных на обеспечение информационной безопасности. На практике под этим подразумевается поддержание определенной целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных.

Информационная безопасность - это защита информации и поддерживающей инфраструктуры от случайных или направленных воздействий естественного или искусственного характера, нанесением ущерба владельцам или пользователям таких данных и использующей инфраструктуры.

Безопасность информационной системы - это признак, заключающее в умении системы обеспечить ее качественное функционирование, то есть обеспечить целостность и скрытность такой информации. Для установления целостности и конфиденциальности данных необходимо обеспечить защиту информации от случайного определенного уничтожения или несанкционированного доступа к нему. Под целостностью надо понимать невозможность несанкционированного или случайного уничтожения, а также модификации информации. Под конфиденциальностью информации - невозможность утечки и несанкционированного завладения хранящейся в ней, передаваемой или принимаемой информации.

Известны следующие источники угроз безопасности:

– антропогенные источники, вызванные случайными или преднамеренными действиями субъектов;

– источники, приводящие к отказам и сбоям технических и программных служб из-за старых программных и аппаратных средств или неисправностей в ПО;

– стихийные источники, вызванные природными условиями или форс-мажорными обстоятельствами.

Есть много возможных направлений утечки информации и путей злоумышленного доступа к ней в сетях:

– перехват данных;

– модификация данных;

– подмена любого авторства информации (кто-то может послать письмо или документ от вашего имени);

– использование минусов операционных систем и прикладных программных средств;

– копирование множества носителей информации и файлов с преодолением мер защиты;

– незаконное подключение к аппаратуре и линиям связи;

– маскировка под зарегистрированного сотрудника и присвоение его полномочий;

– введение новых пользователей;
– внедрение операционных вирусов и так далее.

Для обеспечения безопасности информационных систем применяют системы защиты информации, которые представляют собой комплекс организационно - технологических мер, программно - технических средств и правовых норм, направленных на противодействие источникам угроз безопасности информации.

Защита информации в компьютерных сетях

Локальные сети предприятий очень часто подключаются к сети Интернет. Для защиты локальных сетей корпораций, как правило, применяются межсетевые экраны - брандмауэры (firewalls). Экран (firewall) - это служба разграничения доступа, которое позволяет разделить корпоративную сеть на две части (граница проходит между локальной корпоративная сетью и корпоративная сетью Интернет) и сформировать определенные правила, показывающие условия прохождения пакетов из одной части в другую. Экраны могут реализованы как аппаратными средствами, так и программными.

Защита информации от компьютерных вирусов

Компьютерный вирус - это маленькая вредоносная программа, которая самостоятельно может создавать свои копии и внедрять их в различные программы, документы, загрузочные сектора носителей данных и распространяться по каналам связи.

В зависимости от среды обитания основными типами компьютерных вирусов являются:

– Программные (поражают файлы с расширением .COM и .EXE) вирусы.
– Загрузочные вирусы.
– Макровирусы.
– Сетевые вирусы.

Для моего предприятия я решил взять антивирусную программу NOD32 Antivirus Business Edition

Лучшая безопасность - это безопасность, обеспеченная заранее. Защита от вредоносных программ должна производиться в реальном времени в момент атаки. В любой момент, пока вы ждете обновления вирусных сигнатур, в системе может открыться "окно уязвимости", что может привести к разрушительным последствиям. Технология ThreatSense® антивируса Eset NOD32 закрывает "окно уязвимости", в то время как другие антивирусные программы оставляют его открытым до получения вирусных сигнатур.

Дополнительная данные:

Высокая производительность.

Эффективное обнаружение вредоносных программ не обязательно должно замедлять работу компьютера. NOD32 по большей части написан на языке ассемблера и неоднократно выигрывал награды за высочайшую производительность среди антивирусных программ. NOD32 в среднем в 2-

5 раз быстрее, чем его конкуренты (источник: Virus Bulletin). С переходом на NOD32 производительность вашей системы повысится.

Малое влияние на системные ресурсы.

NOD32 экономит объем жесткого диска и оперативной памяти, оставляя их для критических приложений. Файл установки занимает всего 8,6 Мбайт, а приложению требуется менее 20 Мбайт оперативной памяти (это значение может варьироваться с изменением технологии обнаружения). Обновления технологии ThreatSense, включающие записи эвристической логики и вирусные сигнатуры, обычно имеют объем 20-50 Кбайт. Переход на NOD32 поможет сохранить ценные системные ресурсы.

Простота управления.

Обновления программы и вирусной базы данных выполняются автоматически в фоновом режиме. Если NOD32 применяется на личном или корпоративном компьютере, можно включить возможность автоматического обновления и больше никогда о этом не вспоминать. Предприятия и организации с крупными распределенными сетями могут использовать мощный элемент удаленного администрирования (Remote Administrator), позволяющий разворачивать, устанавливать, наблюдать и контролировать тысячи рабочих станций и серверов NOD32. NOD32 обеспечивает максимальную защиту при минимальном потреблении ресурсов и высочайшей скорости работы.

Модули:

Централизованное управление резидентными антивирусными модулями и фильтрами.

Интуитивная древовидная структура, включающая управление следующими объектами:

- Модуль автоматических обновлений через Internet/LAN;
- Централизованная система log файлов для всех установленных модулей;
- AMON - резидентный on-access монитор;
- NOD32 - on-demand сканер;
- IMON - Internet монитор - сканирующий всю входящую почту по POP3 протоколу;
- EMON - дополнительный модуль сканирования e-mail - сканирует электронную почту, входящую через MAPI интерфейс;
- Гибкий планировщик задач;
- Карантин зараженных файлов;
- Ключевая данные о системе.

7. Разработка структурированной кабельной системы (СКС)

СКС предоставляет собой кабельную систему организации помещения или группы зданий, разделённую на подсистемы. Она выполнена из набора медных и оптических кабелей, кро-панелей, соединительных шнуров, кабельных разъёмов, модульных гнезд, информационных розеток и вспомогательного оборудования. Все перечисленные элементы интегрируются в единую систему и эксплуатируются согласно определённым правилам.

Будет использован **100Base-T.**

100BASE-TX — физический интерфейс Ethernet, позволяющий компьютерам соединятся при помощи кабеля типа «витая пара» *(twisted pair).* Название **100BASE-TX** исходит от некоторых свойств физической основы (кабеля). «100» ссылается на скорость передачи данных в 100 Мбит/с.

Характеристики кабеля:

– Диаметр проводников 0.4-0.6 мм (22-26 AWG), 4 пары (8 проводников, из которых для 100BASE-TX используются только 4). Кабель должен иметь категорию 3 или 5 и качество data grade

– Максимальная длина: 100 метров

– Приемлемые разъемы: 8 контактные RJ-45

Для соединения устройств стандарт 100Base-TX предусматривает использование провода имеющего две пары: одну для передачи, другую — для приема.

Используются две разводки кабеля в порту. MDI для DTE (Data Terminal Equipment) устройств (компьютеры, принтеры и т.д.) и MDI-X для хабов.

При подключении MDI порта к MDI-X порту применяется прямая разводка кабеля. А при соединении передачи с приемом одинаковых портов MDI и MDI или MDI- X и MDI-X применяется "перевернутая" (crossover) разводка кабеля. При этом "передача" соответственно соединяется с "приемом".

Коммутационные розетки

На рабочем месте смонтированы два типа розеток, обеспечивающие минимальные ресурсы рабочего места:

- RJ-45 категории 5 или выше;
- Многомодовое оптоволокно;

Все розетки маркируются

8. Выбор сетевого оборудования. Определение физической структуры сети. Разработка спецификации на корпоративная сеть

Сервер

Сервер IBM BladeCenter LS22

Blade-сервер от компании Intel -сочетание отличного качества и новых технологий.

Сервер IBM BladeCenter LS22 - это многопроцессорный blade-сервер, оснащенный четырехъядерными процессорами, который определенно обеспечивает высокую определяющие производительность системы для работы приложений, интенсивно использующих память. **Сервер IBM BladeCenter LS22** - это глобальное решение для задач, выполняемых и в 2-процессорной, и в 4- процессорной системе. Это обеспечивает еще очень большую производительность и расширяет возможности.

Т а б л и ц а 8.1 - Технические характеристики сервера

Процессор	Четырехъядерный процессор AMD Opteron серии 2000, включая модели со стандартным энергопотреблением и высокоэффективные модели
Количество процессоров (стандартно/максимум)	1/2
Кэш-память (макс.)	2 МБ общей кэш-памяти (второго уровня (L2)) и 2 МБ или 6 МБ общей кэш-памяти третьего уровня
Память(макс.)	До 64 ГБ памяти Double Data Rate (DDR) II Very Low Profile (YLP) (до 800 МГц)
Внутренние жесткие диски	До двух жестких дисков SAS либо твердотельных дисков на каждом blade- сервере (поддержка до 3
Максимальный объем внутренней памяти	734 ГБ с дополнительным модулем SIO
Сетевой интерфейс	2 встроенных двухпортовых контроллера Gigabit Ethernet (GbE)
Модернизация системы ввода-вывода	1 разъем расширения PCI-X и 1 один разъем расширения PCI-Express
Размеры	3 0-миллиметровый двухпроцессорный blade-сервер
Оборудование для управления системами	3 О-миллиметровый двухпроцессорный blade-сервер
Макс. количество blade-серверов на шасси	BladeCenter E 14, BladeCenter H 14, BladeCenter S 6, BladeCenter T 8, BladeCenter HT 12

Поддерживаемые операционные системы	Red Hat Linux®, SUSE Linux, Microsoft® Windows® Server, Windows Small Business Server, IBM ОС 4690
Ограниченная гарантия	Трехлетняя гарантия на заменяемые заказчиком модули и обслуживание на месте эксплуатации

Рабочие станции

Для рабочих станций я предлагаю Моноблок Asus Eee Top ET1611PUT-B0120 по следующим причинам:

- Цена.
- Компактность.
- Производительность.
- Мобильность.

Основные характеристики моноблока Asus Eee Top ET1611PUT-B0120:

Таблица 8.2 - Основные характеристики моноблока

Корпус	"все-в-одном" - черный встроенные устройства:- USB / аудио панель- USB панель- WEB камера- ЖК дисплей- индикаторная панель- панель управления- система охлаждения- устройство для считывания флэш карт
Процессор	Intel Atom D425 1.8 ГГц • socket 599 • Pineview (1 x ядерный) кеш память: 56 кБ (level 1) \ 512 кБ (level 2) особенности архитектуры:- Direct Media Interface- Execute Disable Bit- Hyper-Threading Technology- Integrated single-channel DDR2/DDR3 memory controller- On-chip graphics controller- Streaming SIMD (SSE)- Streaming SIMD Extensions 2 (SSE2)- Streaming SIMD Extensions 3 (SSE3)- Supplemental Streaming SIMD Extension 3 (SSSE3)- технология 64-разрядной адресации памяти (EM64T)
Материнская плата	на основе чипсета Intel NM10 Express
Оперативная память	PC6400 DDR2 SDRAM • 2 ГБ (расш. до 2 ГБ)• 1 x 200-конт. SO-DIMM
Контроллер устройств хранения	• Serial ATA II
Жесткий диск	250 ГБ • Serial ATA II • 5400 об./мин.
Дисплей	15.6" сенсорный ЖК-дисплей • 1366 x 768
Видео	Intel Graphics Media Accelerator 3150 - встроен. - 2048 x 1536 / 16 млн. - совместно используемая SDRAM

Звук	встроен. • стерео • 24-бит. • 3 Вт (RMS) поддерживаемые стандарты:- Intel High Definition Audio (Azalia)
Сетевой адаптер	встроенный сетевой адаптер тип сети:- Ethernet- Fast Ethernet- Gigabit Ethernet скорость передачи данных:- 10 Мбит/сек.- 100 Мбит/сек.- 1000 Мбит/сек. сетевые стандарты:- IEEE 802.3 (Ethernet)- IEEE 802.3ab (TP Gigabit Ethernet)- IEEE 802.3u (Fast Ethernet)
Беспроводная корпоративная сеть	- встроен. Wi-Fi сетевые стандарты:- IEEE 802.11b- IEEE 802.11g- IEEE 802.11n
Операционная система	Microsoft Windows 7 Professional
Устройства ввода Интерфейсы	ASUS U2000 Black USB (клавиатура, мышь), сенсорный экран 2 x USB 2.0 • Тип A • (левая боковая панель) слот для карт памяти SD / MMC • (левая боковая панель) VGA • HD-15F • (задняя панель) последовательный • DB-9M • (задняя панель) 2 x USB 2.0 • Тип A • (задняя панель) электропитание • (задняя панель) Ethernet 10/100/1000BaseT • RJ-45 • (задняя панель) микрофон • мини 3.5мм моно • (задняя панель) наушники • мини 3.5мм стерео • (задняя панель)
Технические характеристики Электропитание	внешн. адаптер питания • 100 / 240 В (перемен. ток) • 40 Вт (номинальная мощность)
Размеры, вес	40.7 x 33.6 x 4.2 см, 3.1 кг

Т а б л и ц а 8.3 - Коммутатор Cisco WS-C3560X-48T-S

Общие характеристики	
Возможность установки в стойку	есть
Количество слотов для дополнительных интерфейсов	4
Объем оперативной памяти	256 Мб
Объем флеш-памяти	128 Мб

LAN	
Количество портов коммутатора	48 x Ethernet 10/100/1000 Мбит/сек
Поддержка работы в стеке	есть
Внутренняя пропускная способность	160 Гбит/сек
Размер таблицы MAC адресов	4096
Управление	
Консольный порт	есть
Web-интерфейс	есть
Поддержка Telnet	Есть
Статическая маршрутизация	есть
Протоколы динамической маршрутизации	IGMP v1, IGMP v2, RIP v1, RIP v2

9. Технико – экономическое обоснование

Описание работы и обоснование необходимости

Поставщики услуг испытывают огромную потребность в привлечении новых пользователей и увеличении среднего дохода от одного абонента.

Пользователям предлагается большой выбор вариантов для удовлетворения потребностей в коммуникациях, развлечениях и информацией, в связи с чем их лояльность одной компании или услуге значительно ослабевает. В попытке найти новые источники доходов и привлечь к себе пользователей поставщики традиционных телекоммуникационных услуг применяют новые нормы и технологии, позволяющие успешно конкурировать непосредственно с поставщиками услуг кабельного телевидения. В результате они приступают к реализации планов предоставления полного набора услуг "три в одном" (Triple Play) по широкополосным сетям следующего поколения.

Описываемая бизнес-модель предназначена для расчета расходов и доходов при внедрении унифицированной сети. Бизнес-модель можно рассматривать лишь в качестве примера развертывания сети. При прогнозировании будущего развития нельзя исключить некоторую неопределенность.

Цель проекта

Целью проекта является разработка и проектирование корпоративной сети. Так как мультислужбаная корпоративная сеть ещё не существует, то основные затраты оператора будут тесно связаны определенно с закупкой специализированного оборудования передачи данных, аренды оптических каналов и заработной платы специалистов.

Маркетинг

Проектируемая корпоративная сеть и услуги ею предоставляемые ориентированы прежде всего на частных пользователей. Основными потребителями такх услуг должны стать абоненты, подписывающиеся на услуги для домашнего использования. Также предоставляются услуги юридическим лицам.

Финансовый план

Назначение данного раздела заключается в прогнозной оценке экономической эффективности проекта на основе анализа притоков и оттоков денежных средств. Финансовый план составляют сроком на три-пять лет.

Этот раздел бизнес-плана является расчётным. Финансовый план включает: расчет величины, определение источника инвестиций, прогноз объема реализации, доходы от продажи товаров или услуг, издержки, прибыль.

Расчёт инвестиционных затрат

Капитальные вложения включают в себя стоимость оборудования, монтажных работ и транспортных услуг.

Строительство гражданских сооружений не предусматривается, так как разработанное устройство будет располагаться в существующем здании, на площади пригодной для размещения устройства данного типа и отвечающей требуемым нормам.

Общие капитальные вложения рассчитываются по формуле:

$$\Sigma К = К_{обор} + К_{мон} + К_{тр} + К_{пр}, \quad (9.1)$$

где Кобор – капитальные вложения на приобретение оборудования

Кмонт - капитальные вложения на монтажные работы;

Ктр - капитальные вложения на транспортные расходы (10% от стоимости оборудования).

$К_{пр}$ – капитальные вложения на проектирование сети

Закупка оборудования осуществляется по ценам представленным в таблице 9.1.

Т а б л и ц а 9 . 1 – Стоимость оборудования

Наименование оборудования	Кол-во оборудования, шт.	Цена оборудования, тыс.тенге. (без НДС)	Общая стоимость с без НДС, тыс.тенге.	НДС, %	Общая стоимость с учетом НДС, тыс.тенге.
Маршрутизатор Cisco 7201-NPE-G2	5	1749,88	8749,4	12	9799,328
Маршрутизатор CISCO7604	20	330,75	6615	12	7408,8
Коммутатор Cisco ME4924-10GE	15	3205,647	48084,705	12	53854,8696
Коммутатор Linksys SPS224G4	720	37,338	26883,36	12	30109,3632
Какбель экранированный Ethernet STP, км	75	120	9000	12	10080
Стоимость всего оборудования, тыс. тенге			99332,465		111252,3608

Стоимость монтажа составляет 10% от стоимости оборудования, и рассчитывается по формуле:

$$К_{МОНТ} = 0{,}1 \cdot К_{ОБОР}, \text{ тыс. тг.} \quad (9.2)$$

И составит:

$$К_{МОНТ} = 0{,}1 \cdot 99332{,}465 = 9933{,}247 \text{ тыс. тг.}$$

Стоимость транспортировки составляет 10% от стоимости оборудования, и рассчитывается по формуле

$$K_{TP} = 0{,}1 \cdot K_{OБОР}, \text{ тыс. тг.} \quad (9.3)$$

И составит:

$K_{TP} = 0{,}1 \cdot 99332{,}465 = 9933{,}247$ тыс. тг.

Расчет капитальных вложений на проектирование сети

$КВ_{пр} = ФОТ + С + А + Э + Н$

где, ФОТ – фонд оплаты труда;
С – стоимость оборудования;
А – затраты на амортизацию;
Э – затраты на электроэнергию;
Н – затраты на налоги.

Затраты на оплату труда зависят от количества задействованных сотрудников и их необходимой квалификации (подразделение ПД). В таблице 9.2 приведена заработная плата сотрудников и их количество в подразделении.

Таблица 9.2 - Оплата труда производственного персонала.

Наименование должностей и профессий	Всего человек	Месячный оклад, тыс.тенге	Основная заработная плата работников в месяц, тыс.тенге
Руководитель	1	170	170
Инженер-проектировщик	1	120	120
Инженер-оператор	3	100	300
Инженер-техник	3	100	300
Консультант по Экономике	1	80	80
Консультант по части БЖД	1	80	80
Менеджер по рекламе	1	80	80
Итого	10		1 130

Заработная плата каждого работника за один рабочий день равна месячному окладу работника, поделенному на количество рабочих дней за прошедший месяц (это 24 дня – шестидневная рабочая неделя):
Для руководителя:

$$D = \frac{170000}{24} = 7083{,}33 \text{ тенге/день;}$$

Инженер-проектировщик:

$$D = \frac{120000}{24} = 5000 \text{ тенге/день;}$$

Инженер-оператор:

$$D = \frac{100000}{24} = 4166{,}66 \text{ тенге/день;}$$

Инженер-техник:

$$D = \frac{100000}{24} = 4166{,}66 \text{ тенге/день;}$$

Консультант по Экономике:

$$D = \frac{80000}{24} = 3333{,}33 \text{ тенге/день;}$$

Консультант по части БЖД:

$$D = \frac{80000}{24} = 3333{,}33 \text{ тенге/день;}$$

Менеджер по рекламе:

$$D = \frac{80000}{24} = 3333{,}33 \text{ тенге/день;}$$

Расходы по заработной плате определяются по следующей формуле:

$$\text{ФОТ} = \text{ФОТ}_{\text{осн}} + \text{ФОТ}_{\text{доп}} \quad (9.4)$$

Основная заработная плата определяется по следующей формуле:

$$\text{ФОТ}_{\text{осн}} = ЗП \cdot 155 \quad (9.5)$$

Составляет:

$\text{ФОТ}_{\text{осн}}$=$ЗП_1$*155+ $ЗП_2$*155+ $ЗП_3$*155+ $ЗП_4$*155+ $ЗП_5$*155+ +$ЗП_6$*155+ $ЗП_7$*155=7083,33*155 + 5000*155+4166,66*155+4166,66*155+3333,33*155+ +3333,33*155+3333,33*155=10 268 тыс.тг

В годовой фонд оплаты труда включается дополнительная заработная плата (работа в праздничные дни), в размере 10% от основной заработанной платы:

$$ФОТ_{доп} = Ф_{осн} \cdot 0{,}1, \quad (9.6)$$

Составляет:

$$ФОТ_{доп} = 10\,268 \cdot 0{,}1 = 1026$$

В соответствии с формулой 3.8 фонд оплаты труда составит:

ФОТ = 10 268 тыс. тг. + 1 026 тыс. тг. = 11 294 тыс. тг.

Отчисления на социальный налог составляет 11% от ФОТ с учетом выплат в пенсионный фонд, и вычисляются по формуле:

$$O_{сн} = (ФОТ - ПФ) \cdot Нсн \quad (9.7)$$

где ПФ – отчисления в пенсионный фонд, которые рассчитываются по формуле:

$$ПФ = ФОТ \cdot 0{,}1 \quad (9.8)$$

Составляет:

ПФ = 11 294 · 0,1 = 1 129

Тогда:

$О_{сн}$= ФОТ· 0,11= (11 294 - 1129) · 0,11 = 11 169,81 тыс.тг.

Расчет затрат на амортизацию

На данную систему связи по существующему положению в настоящее время норма амортизации $Н_А$ на оборудование составляет 25% от стоимости всего оборудования. Таким образом амортизационные рассчитываются по формуле:

$$A = (\frac{H_A \cdot K_{ВЛ}}{365 \cdot 100\%}) \cdot 155 \quad (9.9)$$

Составляют:

$$A = (\frac{25\% \cdot 99332{,}465}{365 \cdot 100\%}) \cdot 155 = 10545{,}569 \text{ тыс. тенге}$$

Расчет затрат на электроэнергию

Затраты на электроэнергию для производственных нужд, включают в себя расходы электроэнергии на используемое оборудование и дополнительные и вычисляются по формуле:

$$З_{эл.эн} = З_{эл.эн.обор} + З_{доп.нуж}, \text{ где} \quad (9.10)$$

где $З_{эл.эн.обор}$ – расходы электроэнергии оборудованием.

$З_{доп.нуж}$ – расходы электроэнергии на дополнительные нужды.

Расходы электроэнергии оборудованием рассчитываются по формуле

$$З_{эл.эн.обор} = W \cdot T \cdot S, \text{ где} \quad (9.11)$$

где W – потребляемая мощность,

T – время работы, (T=1240 ч)

S – тариф (S= 14 тг/кВт).

$З_{ЭЛ.ЭН.ОБОР.-1} = 0{,}9 \cdot 1240 \cdot 14 \cdot 0{,}9 = 14061{,}6$ тенге;

$З_{ЭЛ.ЭН.ОБОР.-2} = 0{,}5 \cdot 1240 \cdot 14 \cdot 0{,}9 = 7812$ тенге;

Сумма затрат на электроэнергию основного оборудования составляют:

$З_{ЭЛ.ЭН.ОБОР.} = 14061{,}6 + 7812 = 21873{,}6$ тенге;

Затраты на дополнительные нужды составят:

$З_{ДОП.НУЖ.} = 5\% \cdot 21873{,}6 = 1093{,}68$ тенге;

Итого затраты на электроэнергию составляют :

$Э = 21873{,}6 + 1093{,}68 = 22877{,}28$ тенге;

Расчет затрат на накладные расходы

Прочие затраты на производственные, транспортные, управленческие и эксплуатационно-хозяйственные определенные расходы определяются укрупнено в размере 10% от общей суммы затрат.

$$H_P = (ФОТ + A + З_{ЭЛ.ЭН} + O_{СН}) \cdot 75\%, \quad (9.12)$$

И составляют:

$Н_Р$ = (11 294 + 24833,11625 + 22877,28 + 1476,684)·75% = 53149,92837 тыс. тенге

Капитальные расходы согласно формуле 3.7 составляют:

$К_1$ = 11 294 + 99332 + 22877,28 + 10545,684 + 53149,93 = 196 198,9 тыс. тенге

Расчёт инвестиционных затрат 2-ым способом

Общие капитальные вложения рассчитываются по формуле:

$$\Sigma К = К_{обор} + К_{мон} + К_{тр} + К_{пр}, \quad (9.13)$$

где, Кобор – капитальные вложения на приобретение оборудования

Кмонт - капитальные вложения на монтажные работы;

Ктр - капитальные вложения на транспортные расходы (10% от стоимости оборудования).

$К_{пр}$ – капитальные вложения на проектирование сети

Закупка оборудования осуществляется по ценам представленным в таблице 9.4

Т а б л и ц а 9 . 4 - Стоимость оборудования

Наименование оборудования	Кол-во оборудования, шт.	Цена оборудования, тыс.тенге. (без НДС)	Общая стоимость с без НДС, тыс.тенге.	НДС, %	Общая стоимость с учетом НДС, тыс.тенге.
Маршрутизатор Cisco 7201-NPE-G2	5	1949,88	9749,4	12	10799,328
Маршрутизатор CISCO7604	20	390,75	9815	12	10808,8
Коммутатор Cisco ME4924-10GE	15	3505,647	52584,705	12	63101,8696
Коммутатор Linksys SPS224G4	720	40,338	28883,36	12	34109,3632
Кабель экранированный Ethernet STP, км	75	150	11250	12	13580
Стоимость всего оборудования, тыс. тенге			122281,23		142397,3608

Стоимость монтажа составляет 10% от стоимости оборудования, и рассчитывается по формуле:

$$K_{МОНТ} = 0{,}1 \cdot K_{ОБОР},\ \text{тыс. тг.} \qquad (9.14)$$

И составит:

$K_{МОНТ} = 0{,}1 \cdot 122281{,}23 = 12228{,}123$ тыс. тг.

Стоимость транспортировки составляет 10% от стоимости оборудования, и рассчитывается по формуле

$$K_{ТР} = 0{,}1 \cdot K_{ОБОР},\ \text{тыс. тг} \qquad (9.15)$$

И составит:

$K_{ТР} = 0{,}1 \cdot 122281{,}23 = 12228{,}123$ тыс. тг.

Тогда затраты на амортизацию во 2-ом случае:

$A = (\frac{25\% \cdot 122281{,}23}{365 \cdot 100\%}) \cdot 155 = 14981{,}267$ тыс. тенге

Капитальные вложения:

$К_2$ = 11 294 + 99332 + 22877,28 + 14981,267 + 53149,93 = 201 798,9 тыс. тенге

Оценка эффективности капитальных вложений для реализации проекта

Оценка эффективности реализации проекта производится на основе показателя минимума приведенных затрат, который рассчитывается по формуле:

$$З_i = С_i + Е_н * К_i \qquad (9.16)$$

где $С_i$ – эксплуатационные издержки

$К_i$ – капитальные вложения;

$Е_н$ – коэффициент экономической эффективности (15%) .

В качестве такого показателя издержек берется показатель - затраты на амортизацию, все остальные такие показатели издержек в обоих вариантах реализации проекта остаются на одинаковом уровне. Затраты на амортизацию рассчитываются по формуле:

$$A = \frac{\text{Соб} * \text{На}}{100\%}, \qquad (9.17)$$

где $C_{об}$ – стоимость оборудования,
$H_а$ – норма амортизации (25%)

Вариант 1

$$\text{А1} = \frac{99332 * 25\%}{100\%} = 24833 тыс.тенге$$

Вариант 2

$$\text{А2} = \frac{122281 * 25\%}{100\%} = 30570 тыс.тенге$$

Таким образом, согласно формуле (4.1), приведенные затраты составят:

$З_1 = С_1 + Е_н * К_1 = 24833 + 0,15 * 196198 = 54262,7$ тыс. тенге

$З_2 = С_2 + Е_н * К_2 = 30570 + 0,15 * 201798 = 60839,7$ тыс. тенге

Т.к. $З_1 < З_2$, 1-ый вариант реализации проекта является наиболее эффективным.

Заключение

Оценка эффективности проекта производилась путем расчета минимальных приведенных затрат. Таблица 9.5.

Т а б л и ц а 9 . 5 - Сравнение приведенных затрат

	Вариант 1	Вариант 2
Стоимость оборудования, тенге	99332,5	122281,2
Приведенные затраты $З_i$, тенге	54262,7	60839,7

Для реализации проекта были произведены расчеты для 2-ух вариантов стоимости оборудования.

Согласно таблице, видно, что приведенные затраты для 1-го варианта реализации проекта, меньше приведенных затрат при расчете 2-ым способом, т.е. 1-ый вариант реализации проекта обходится дешевле, следовательно,

использовать расчеты стоимости оборудования 1-го варианта будет эффективнее.

10. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

10.1 Анализ условий труда обслуживающего персонала при эксплуатации технического оборудования

Главной целью данного проекта является «Автоматизация рабочего места Архив».

В список опасных и вредных факторов при работе за компьютером входят:

1) повышенная напряженность электрического поля;
2) токсические вещества;
3) повышенный уровень шума на рабочем месте;
4) пониженная контрастность;
5) повышенная напряженность магнитного поля;
6) недостаточная освещенность рабочей зоны;
7) повышенный уровень статистического электричества.

Касательно здоровья сотрудников, можно выделить несколько факторов риска, которым сопровождается влияние компьютера на организм человека:

1) проблемы, обусловленные наличием электромагнитного излучения;
2) проблемы зрения;
3) проблемы, связанные с мышцами и суставами;
4) стресс, депрессия и другие нервные расстройства, которые обуславливаются влиянием компьютера на психику человека.
5) малоподвижный образ жизни;
6) переработка (более 9 часов в сутки);
7) стрессы;
8) работа в ночное время суток, и как следствие нарушение выработки гормона мелатонина.

Магнитное поле.

Компьютер при работе создает вокруг себя электромагнитное поле, которое имеет способностью биологического специфического и теплового воздействия на организм человека. За счет влияния электромагнитного поля на клетки и ткани человека происходят нарушения условно-рефлекторной деятельности, снижение активности мозга. Все это проявляется в головной боли, утомляемости, ухудшении самочувствия, гипотонии.

За счет теплового воздействия электромагнитного поля повышается температура тела, идет нагрев тканей и органов. Больше всего подвержены

тепловому облучению такие органы как печень, поджелудочная железа, мочевой пузырь, желудок. Все это может вызвать язвы кровотечения и перфорации [30].

Шум.

На рабочем месте сотрудников источниками шума, как правило, являются разговаривающие люди, внешний шум и отчасти – компьютер, принтер. Они издают довольно незначительный шум, поэтому в помещении достаточно использовать звукопоглощение.

Из строительно-акустических методов защиты от шума (СНиП-II-12-77) выбран метод для помещения, представленного на рисунке 1 – план рабочего помещения:

– звукопоглощающие конструкции и экраны.

Для выбранного помещения выбрано звукопоглощающие облицовка состоящая из матов, из супертонкого стекловолокна с оболочкой из стеклоткани, которую нужно разместить на потолке и верхних частях стен. Максимальное звукопоглощение будет достигнуто при облицовке не менее 60 % общей площади ограждающих поверхностей помещения.

Электростатическое поле, вредные вещества в воздухе

При работе компьютер образует вокруг себя электростатическое поле, которое деионизирует окружающую среду, а при нагревании платы и корпус монитора испускают в воздух вредные вещества. Всё это делает воздух очень сухим, слабо ионизированным, со специфическим запахом и в общем "тяжёлым" для дыхания. Естественно, такой воздух не может полезен для организма и может привести к заболеваниям аллергического характера, болезням органов дыхания и другим расстройствам [30].

В чем заключается вред работы ночью.

Мелатонин – основной гормон эпифиза, регулятор суточного ритма. Вырабатывается ночью, и его максимальная концентрация достигается к 5 часам утра. Этот гормон регулирует функции клеточного обновления, нейтрализует разрушительные последствия окислительных процессов, которые являются основной причиной старения и увядания кожи, участвует в защите организма от неблагоприятных воздействий. Мелатонин очень важен для организма, и, поскольку выработка этого гормона происходит преимущественно ночью, то любой сбой сна приводит к снижению его выработки.

Известно, что в организме человека существуют так называемые биологические часы. Причем одни получают информацию о смене дня и ночи напрямую через зрительный канал, а другие – наш внутренний “счетчик времени”.

В нормальном режиме часы работают синхронно. Одни при наступлении темноты запускают “режим сна”, другие синхронно этому запускают соответствующие нейробиологические и гормональные процессы.

Достаточно просто просиживать большое количество времени перед ярким монитором, чтобы гарантированно испытать ослабленный эффект десинхронии. Работая в ночное время мы стимулируем эпифиз ярким светом монитора и вводим в заблуждение наши внутренние часы, которые “рассчитывают” на ночь. Как следствие такой работы – блокировка секреции мелатонина.

Технический персонал состоит четырех сотрудников: три технический специалист по работе с БД «Архив», диспетчер поддержки и отладки работы оборудования. Максимальное количество присутствующих в кабинете сотрудников составляет два человека, это технический специалист по работе с БД «Архив» и диспетчер поддержки и отладки. Так как сервер должен работать круглосуточно, то специалисты по работе с БД работают в три смены, количество рабочих часов составляет 8 часов. График смен специалистов по работе с БД:

- с 8:00 до 16:00 ч.
- с 17:00 до 24:00 ч.
- с 00:00 до 07:00 ч.

Так же они меняются сменами. Они работают с понедельника по субботу. Так же данным сотрудникам выделяеться промежуток в три часа в который они должны успеть принять пищу, учитывая что перерыв длиться 1 час [29].

Сотрудник занимающийся поддержкой и отладкой оборудования работает каждый день, по 8 часов с учетом переыва на обед, который составляет 1 час и он может выбрать время обеда с 12:00 – 15:00. С понедельника по субботу. Выходной день воскресенье [29].

Работа сотрудников непосредственно связана с компьютером, а соответственно с вредным дополнительным воздействием целой группы факторов, что существенно снижает производительность их труда.

К таким факторам можно отнести:

1) неправильная освещенность;

2) нарушение микроклимата;

3) наличие напряжения.

Согласно ГОСТ 12.1.005-88 ССБТ «Оптимальные и допустимые нормы микроклимата, в зависимости от категории работ», работа людей в помещение относится к работе лёгкой тяжести(1а), так как управление оборудованием осуществляется дистанционно с помощью компьютеров

С целью создания нормальных условий для работников предприятий Связи установлены нормы производственного микроклимата. В помещениях при работе с ПК должны соблюдаться следующие климатические условия [30]:

Холодный период года

- оптимальная температура 24 С˚, допустимая температура 26 С˚;
- относительная влажность 45 %, допустимая влажность 60%;
- скорость движение воздуха относительная и допустимая 0,05 м/с;

Тёплый период года

- оптимальная температура 23 С˚, допустимая температура 25 С˚;
- относительная влажность 50 %, допустимая влажность 55%;
- скорость движение воздуха относительная 0,1 м/с и допустимая 0,1 м/с.

Помещение имеет размеры: длина (L) = 7 метров, ширина (B) = 4 метра, высота (H) = 4 метра. Помещение находится в здании на 1-м уровенье, рассчитано на 2 рабочих места.

План помещения выбранного для размещения оборудования и технического персонала изображен на рисунке 10.1.

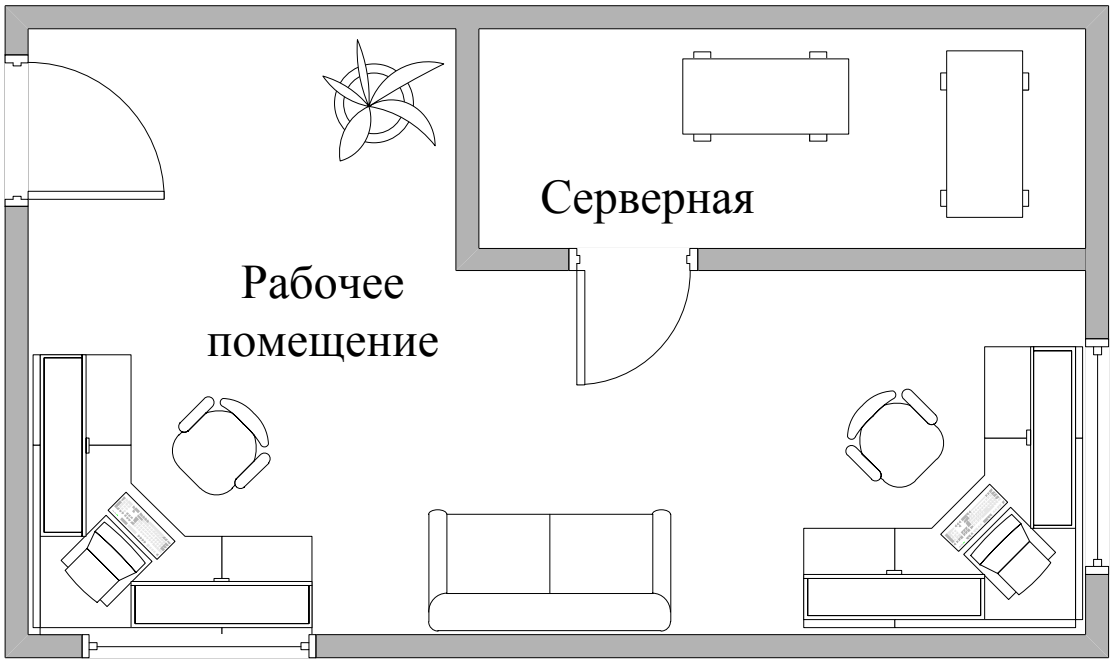

Рисунок 10.1 – План рабочего помещения

Рабочее место состоит из следующих компонентов:
- два стола;
-один двух-местный диван;
- два эргономических стула;
- два персональных компьютера, один из которых является сервером
-Серверной:

1) Intel Core i5 Win 7 (3.4 GHz, 16 GB ОЗУ)
2) Intel Core i7 Win 7 (3.8 GHz, 32 GB ОЗУ)

10.2 Расчет системы искусственного освещения помещения

Помещение зала имеет естественное освещение через 3 боковых окно, и искусственное освещение, которое позволяет вести работы в темное время суток и днем в местах, где показатель КЕО не соответствует нормативам.

Поэтому рассчитаем общее освещение помещения аппаратного зала длиной А = 7 м., шириной В = 4 м., высотой Н = 4 м. Так как ориентация окон в предложенном плане помещения(Рисунок 1): Для первого окна (слева) южная и для второго окна (справа) юго-восточная то стены будут окрашены в светло-голубой, пол будет зеленый. Так как работа будет связана с компьютерами то коэффициент отражения будет составлять:

1. для потолка: 60%;
2. для стен: 40%;
3. для пола: 30%;
4. Для других поверхностей и рабочей мебели: 32%.

Разряд зрительной работы – III высокой точности. Нормируемая освещенность – 400 лк. [28]. Для помещения используем люминесцентную лампу ЛБ (белого цвета), мощностью 40 Вт., световым потоком 3300 лм., диаметром 40 мм. и длиной со штырьками 1210,6 мм [31].

Высота светильника h_c = 4-r, где r- высота лампочки

h_c = 4- 3,2 = 0,8 м

Высота рабочей поверхности h_P = 1,2 м.

Определим необходимое расстояние между светильниками [31]:

$$L = \lambda \cdot h \text{ м.}, \tag{10.1}$$

где $\lambda = 1.2 \div 1.4$ [28].

Высота светильника над освещаемой поверхностью:

$$h = H - h_P - h_c = 4 - 1{,}2 - 0{,}8 = 2 \text{ м.}, \tag{10.2}$$

По этим данным находим, что необходимое расстояние между светильниками равно:

$$L = \lambda \cdot h = 1{,}2 \cdot 2 = 2{,}4 \text{ м.}, \tag{10.3}$$

Определим индекс помещения I [1]:

$$I = \frac{A \cdot B}{h \cdot (A + B)} = \frac{7 \cdot 4}{3{,}2 \cdot (7 + 4)} = 0{,}795, \tag{10.4}$$

Определим коэффициент использования η [31] .

$$\eta = 0{,}63$$

В качестве светильника возьмем ЛСП02 рассчитанный на две лампы мощностью 40 Вт, диаметром 40 мм и длиной со штырьками 1210,6 мм. Длина светильника 1234 мм, ширина 276 мм. Световой поток лампы ЛБ 40 Фл составляет 3300 лм., световой поток, излучаемый светильником Фсв равен:

$$\Phi_{СВ} = \Phi_{Л} \cdot 2 = 3300 \cdot 2 = 6600 \text{ лм.} \qquad (10.5)$$

Определим число светильников:

$$N = \frac{E \cdot K_З \cdot S \cdot Z}{n \cdot \Phi_{Л} \cdot \eta}, \qquad (10.6)$$

где S – площадь помещения, S=28 м^2.;
КЗ – коэффициент запаса, КЗ=1,5[1];
Е – заданная минимальная освещенность, Е=400 лк. [28];
Z – коэффициент неравномерности освещения, Z=1,2 [28];
n – количество ламп в светильнике, n=2;
Фл – световой поток выбранной лампы, Фл=3300 лм.;
η – коэффициент использования, η=0,63 [28].

$$N = \frac{400 \cdot 1{,}5 \cdot 28 \cdot 1{,}2}{2 \cdot 3300 \cdot 0{,}63} = 4{,}848 \approx 5 \text{ светильников}$$ (Расположение светильников показано на рисунке 10.2)

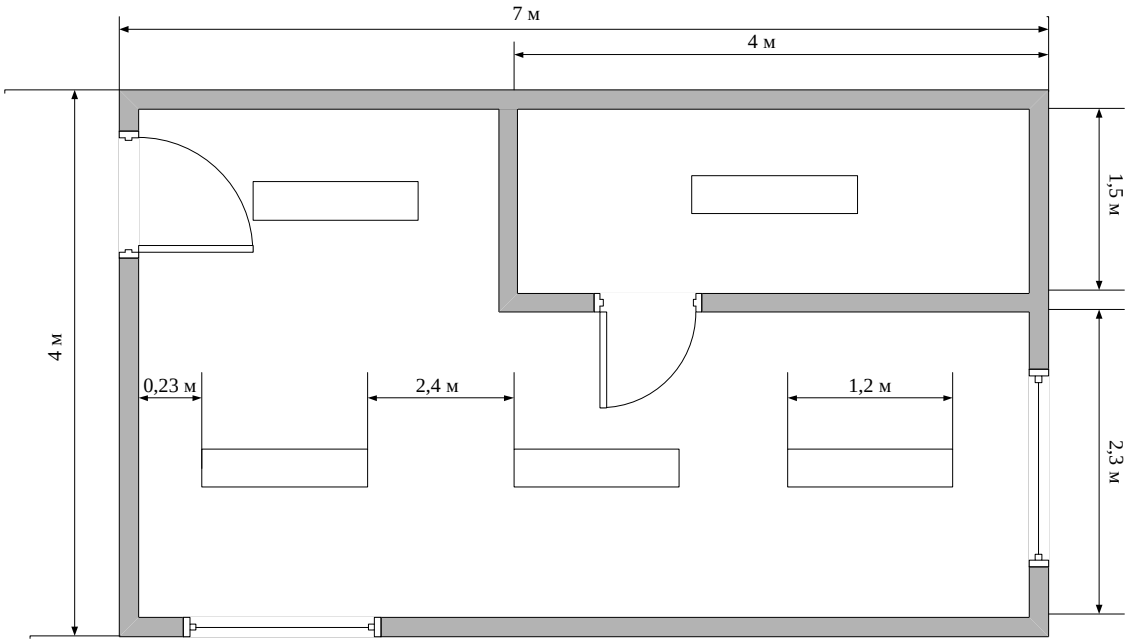

Рисунок 10.2 – Расположение светильников в помещении

Итого, для создания нормированной освещенности нам понадобится 6 ламп в 6-ти светильниках располагающихся в два ряда, в каждом светильнике по одной лампе.

10.3 Анализ пожарной безопасности

Согласно СНиП 2.04.09-84 здание по степени опасности развития пожара, от функционального назначения и пожарной нагрузки горючих материалов, относится к 1-ой группе категории D.

Причинами возникновения пожара могут :

– Возгорание элементов аппаратуры;

– Возгорание отделочных материалов от неисправных выключателей, розеток.

– Несоблюдение режимов эксплуатации оборудования, неправильное действие персонала.

При возникновении пожара может пострадать не только помещение, но и дорогостоящая аппаратура, привести к человеческим жертвам. Поэтому необходимо чтобы были приняты меры по раннему выявлению и ликвидированную пожаров. Источниками зажигания могут оказаться электронные схемы ПК, приборы, применяемые для технического обслуживания, устройства электропитания, кондиционеры воздуха, где в результате различных нарушений образуются перегретые элементы, и др [31].

В соответствии с требованиями правил пожарной безопасности помещение оборудованы углекислотными огнетушителями ОУ-5 с учетом – один огнетушитель на 100 м^2. Общая площадь помещения управления составляет 28 м^2 таким образом устанавливаются 1 огнетушитель. В качестве

огнетушащего вещества применяется комбинированный углекислотно-хладоновый состав. Расчетная масса комбинированного углекислотно-хладонового состава m_d ,кг, для объемного пожаротушения определяется по формуле:

$$m_d = k \cdot g_n \cdot V \tag{10.7}$$

где k = l,2- коэффициент компенсации не учитываемых потерь углекислотно-хладонового состава [31];

g_n = 0,04 – нормативная массовая концентрация углекислотно-хладонового состава [31];

V – объем помещения,

$$V = A \cdot B \cdot H \tag{10.8}$$

Где: A = 7 м – длина помещения,

B = 4 м – ширина помещения,

H = 4 м – высота помещения.

Тогда: V = 7*4*4 = 112 м^3

Следовательно: m_d = 1,2*0,04*112 = 5,376 ≈ 5 кг

Расчетное число баллонов ξ определяется из расчета вместимости в 20-литровый баллон 12 кг углекислотно-хладонового состава.

Внутренний диаметр магистрального трубопровода d_i, мм, определяется по формуле:

$$d_i = 12 * \sqrt{2} = 17\,мм \tag{10.9}$$

Эквивалентная длинна магистрального трубопровода l_2. м, определяется по формуле:

$$l_2 = k_1 * l_2 \tag{10.10}$$

где k_1=1,2-коэффициент увеличения длины трубопровода для компенсации не учитывающих местных потерь [31],

l = 2,7 м – длина трубопровода по проекту тогда [31],

$l_2 = 1{,}2 * 2{,}7 = 3{,}24\,м.$

Расход углекислотно-хладонового состава Q, кг/с, в зависимости от эквивалентной длины и диаметра трубопровода равна 1,5 кг/с

Расчетное время подачи углекислотно-хладонового состава t. мин, определяется по формуле:

$$t = \frac{m_d}{60 * Q} \quad (10.11)$$

Тогда получаем

$$t = \frac{5}{60 * 1{,}5} = 0{,}06$$

Масса основного запаса углекислотно-хладонового состава m, кг, определяется по формуле:

$$m = 1{,}1 * m_d * \left(1 + \frac{k_2}{k}\right) \quad (10.12)$$

где K_2 = 0,2 – коэффициент учитывающий остаток углекислотно-хладонового состава в баллонах и трубопроводах

$$m = 1{,}1 * 5 * \left(1 + \frac{0{,}2}{1{,}2}\right) = 5{,}5 * 1{,}17 = 6{,}435 \text{ кг}$$

Таким образом из полученных результатов можно сделать вывод, что для обеспечения нормального функционирования системы автоматического пожаротушения потребуется 1 баллон углекислотно-хладонового состава вместимостью 20 литров, с массой смеси 6 кг. Нахождение огнетушителя представлено на рисунке 10.3.

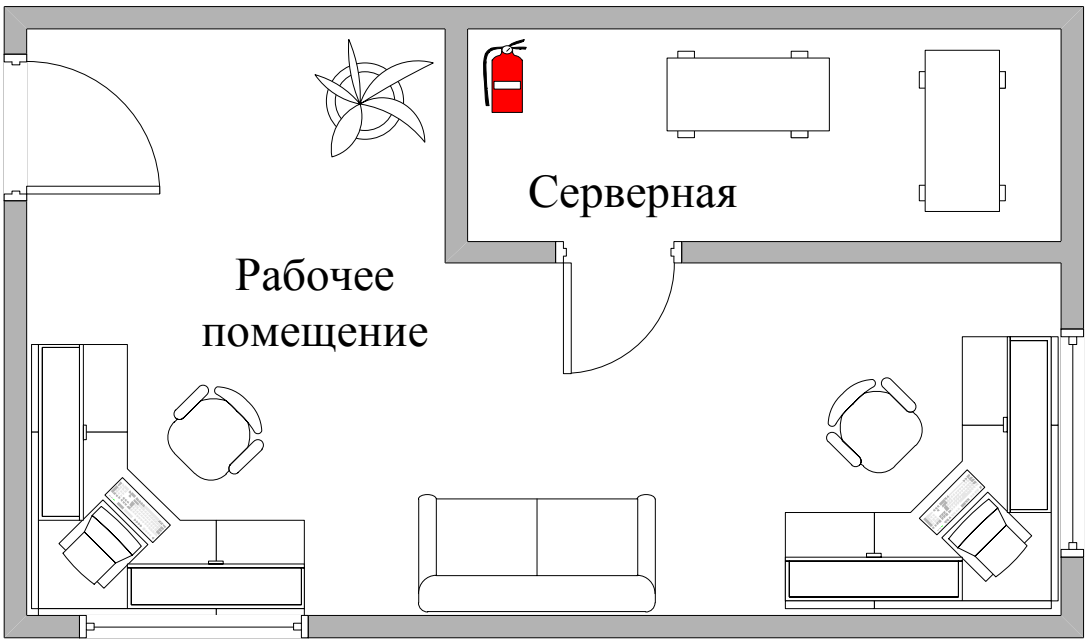

Рисунок 10.3 – Размещение огнетушителя в помещении

10.4 Выводы по безопасности жизнедеятельности.

В данном разделе был произведён анализ условий труда в рабочем помещении для четверых сотрудников. Уровень условий труда признан допустимым, и данные, полученные из расчетов полностью удовлетворяют требованиям стандартов безопасности жизнедеятельности.

Так как в помещение есть два окна, которые в дневное время суток обеспечивают достаточным необходимым количеством света для работы, необходимо было рассчитать освещенность в основном для позднего времени суток. Поэтому для создания нормированной освещенности вечером(ночью) понадобится 6 ламп мощностью 40 Вт., световым потоком 3300 лм., диаметром 40 мм. и длиной со штырьками 1210,6 мм. в 6-ти светильниках, располагающихся в два ряда, в каждом светильнике по одной лампе.

Электротехническое оборудование в помещения является потенциальным источником возникновения и пожароопасности. Из расчетов получили, что для обеспечения нормального функционирования системы автоматического пожаротушения потребуется 1 баллон углекислотно-хладонового состава вместимостью 20 литров, с массой смеси 6 кг.

Заключение

В данном дипломном проекте в программе-эмулятор была создана схема проектируемой корпоративной сети филиала. Создана схема IP-адресаций. Установлен и настроен служба DHCP и протокол NAT. Настроена динамическая маршрутизация с использованием протока OSPF. Произведена настройка коммутаторов, маршрутизаторов, сервера и другого сетевого оборудования.

С развитием современных компьютерных сетей в настоящее время становится важным вопрос об их надежной разработке. От грамотного создания проекта сети зависит её работоспособность и качество связи внутри филиала.

В дипломном проекте найдены оптимальные решения для создания корпоративных сетей подключенных к сети Интернет.

Применение надежного и качественного оборудования при строительстве сети позволило обеспечить высокий уровень стабильности работы всех участков сети. В итоге сотрудники филиала получили доступ к сети Интернет с качеством связи и скоростью соединения превосходящей подключение через аналоговые модемы. Кроме того, корпоративная сеть позволяет пользователям обмениваться программами, аудио и видео записями.

Список литературы

1 Сайт http://corp.alser.kz/page/65/.

2 Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник. - СПб: Изд-во «Питер», 2001. - 672 с.

3 Компьютерные сети. Книга 1: High-Performance Networking. Энциклопедия пользователя: Пер. с англ./Марк А. Спортак и др. - К.: Изд-во «ДиаСофт», 1999. - 432 с.

4 Компьютерные сети. Книга 2: Networking Essentials. Энциклопедия пользователя: Пер. С англ./Марк А. Спортак и др. - К.: Изд-во «ДиаСофт», 1999. -432 с.

5 Новиков Ю. В., Кондратенко С.В. Локальные сети: архитектура, алгоритмы, проектирование. - М.: ЭКОМ, 2001 - 312 с.

6 Гук М. Аппаратные средства локальных сетей. Энциклопедия. - СПб: Изд-во «Питер», 2000. - 576 с.

7 Жаров А., Железо, IBM, 2004.

8 Антон Ленников, учебник: Строим Локальную Корпоративная сеть Ver 2.01. 2004

9 Новиков Ю. В., Кондратенко С. В., Локальные сети: архитектура, алгоритмы, проектирование. - М.: ЭКОМ, 2001.

10 Сводная таблица провайдеров./Журнал Интернет и Я, № 10 (63) 2003, с. 38-39.

11 Сайт http://metod.ce.cctpu.edu.ru/edu/df/pd/book/Modem/classification.

12 Сайт http://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D0%B5%D0%BC%D0%BD%D1%8B%D0%B9_%D0%BF%D1%83%D0%BB.

13 Сайт http://provod.beeline.kz/ru/almaty/tarifs/novye_skorosti.wbp.

ПРИЛОЖЕНИЕ А

Головной Офис (Алматы)

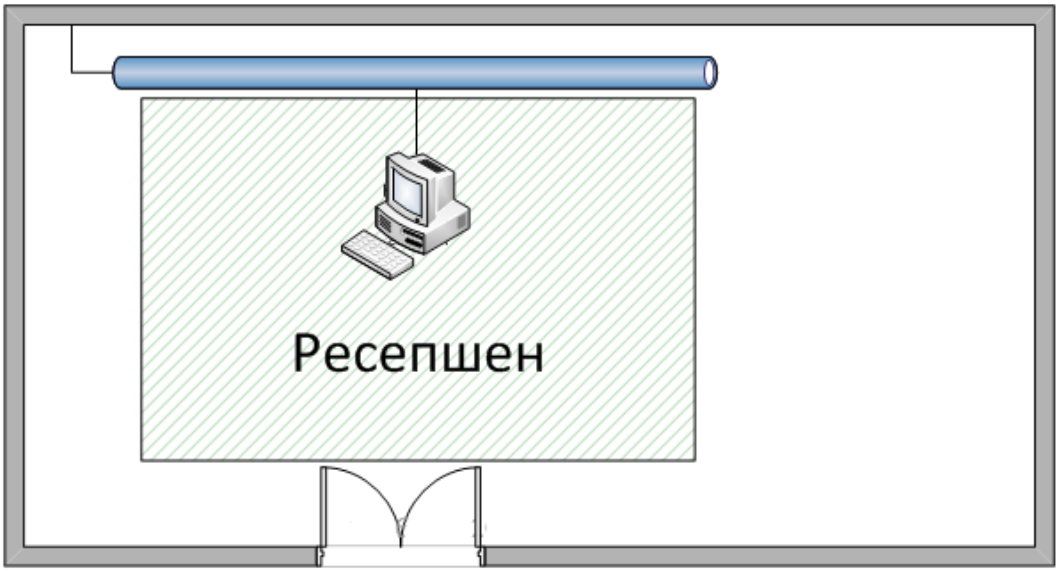

Рисунок 2 – Структура сети головного офиса. Ресепшен

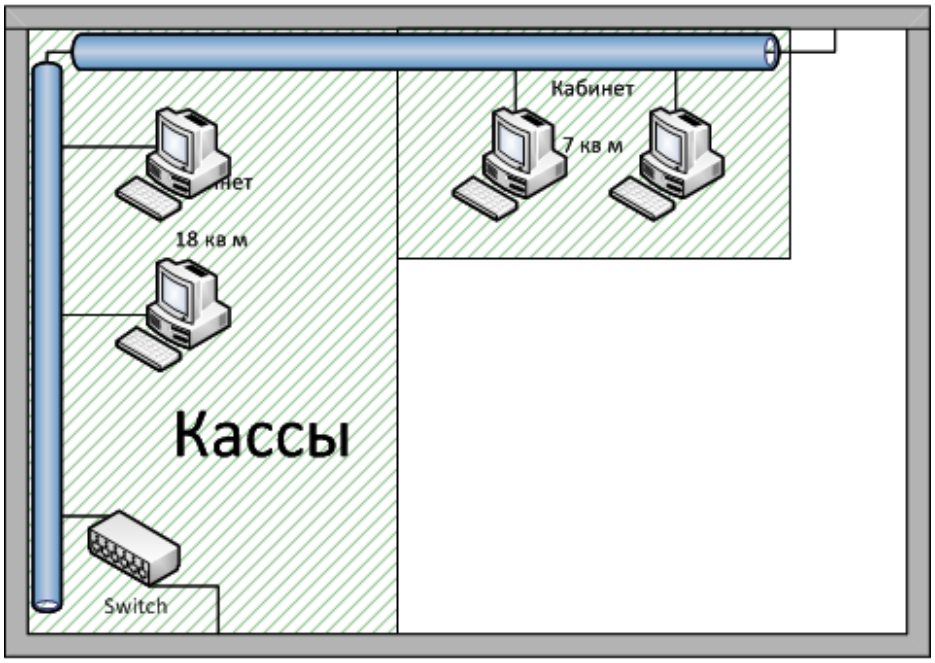

Рисунок 3 – Структура сети головного офиса. Кассы

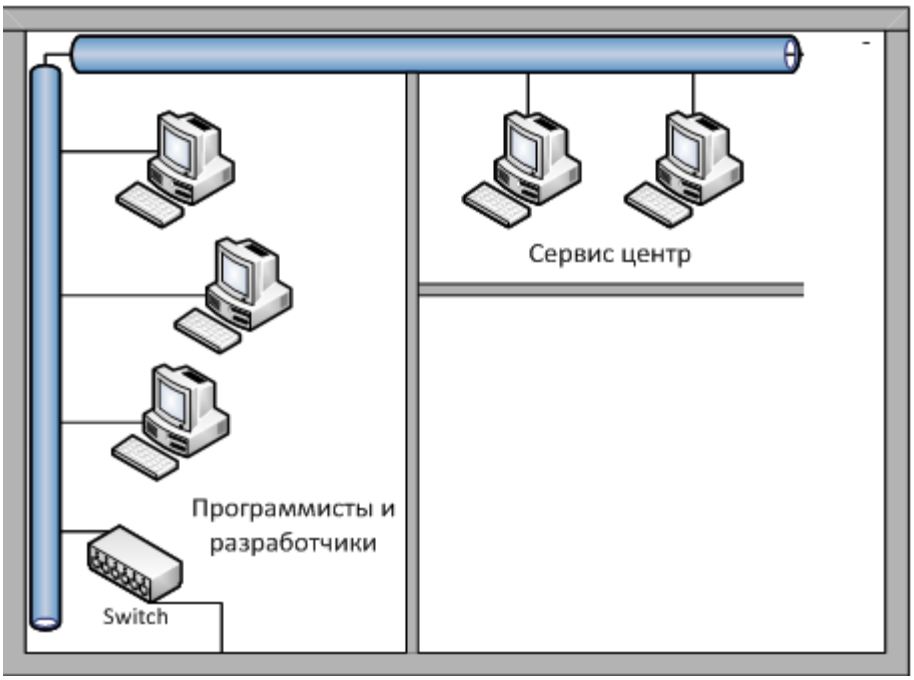

Рисунок 4 – Структура сети головного офиса

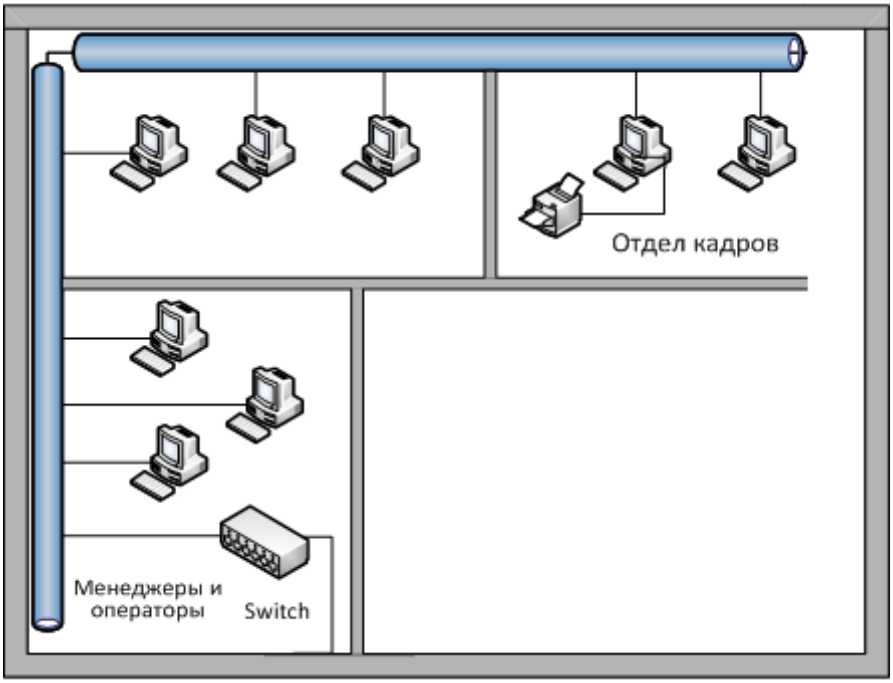

Рисунок 5 – Структура сети головного офиса

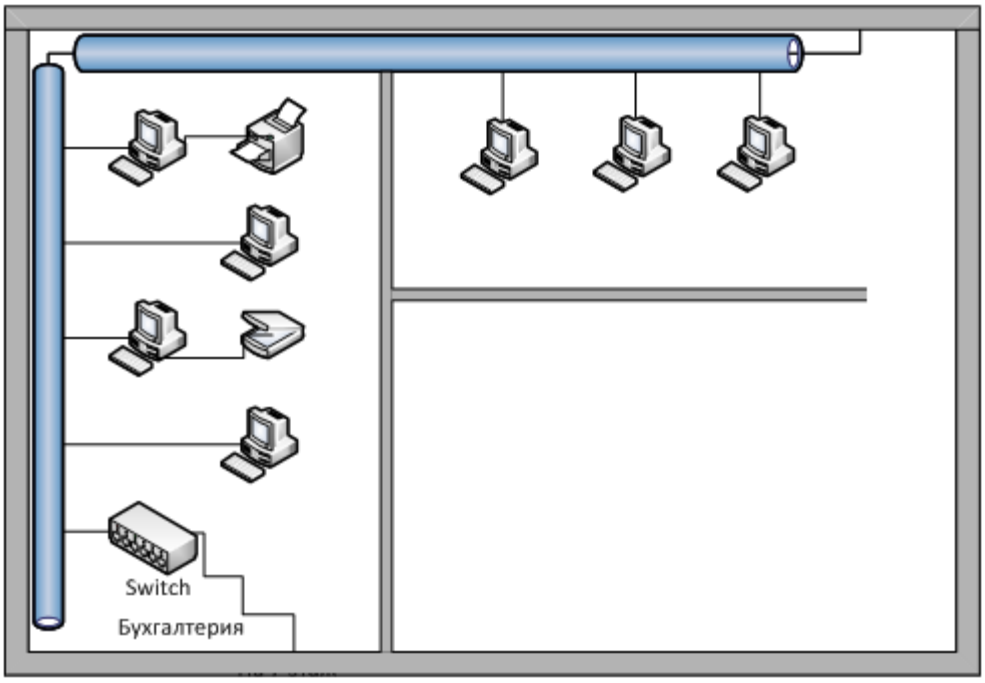

Рисунок 6 – Структура сети головного офиса

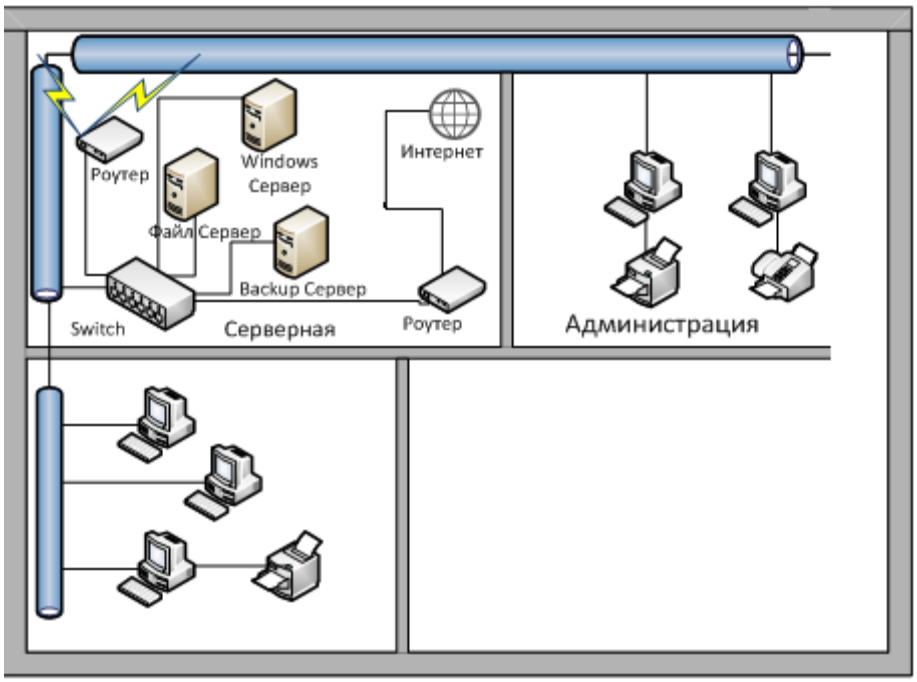

Рисунок 7 – Структура сети головного офиса

ПРИЛОЖЕНИЕ Б

Филиал (Астана)

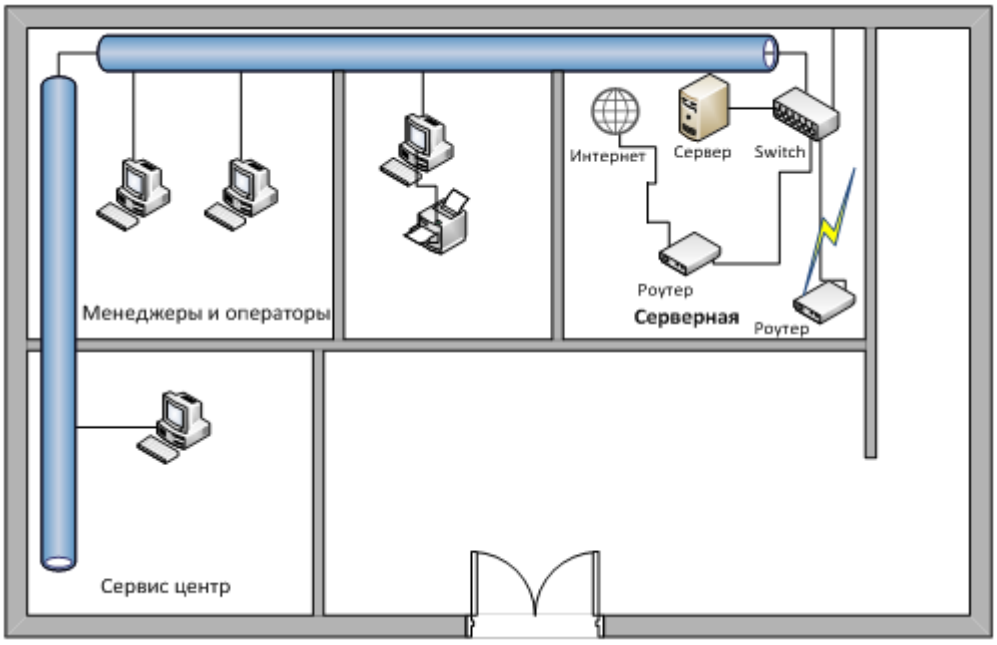

Рисунок 8 – Структура сети филиала в Астане

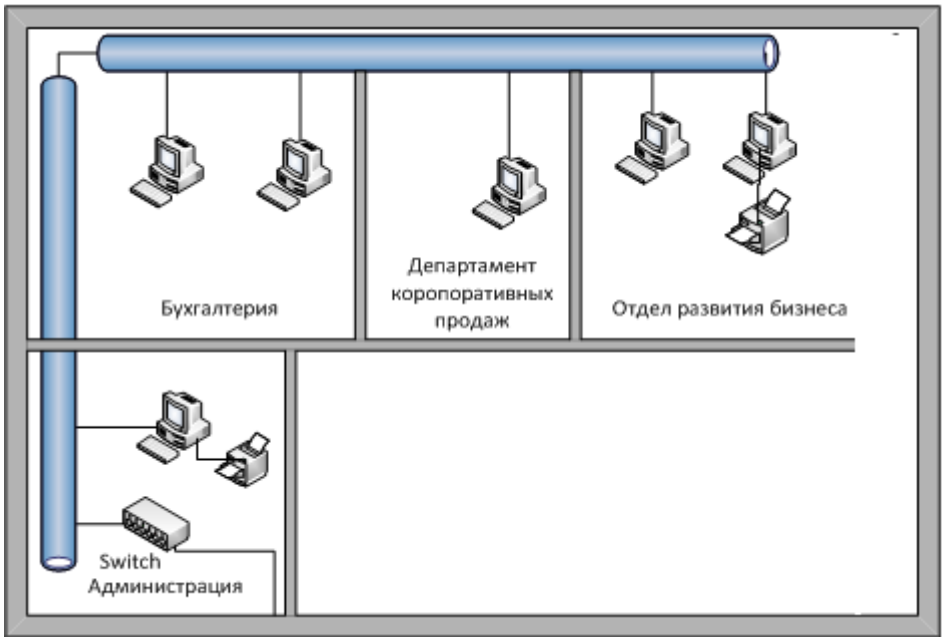

Рисунок 9 – Структура сети филиала в Астане

ПРИЛОЖЕНИЕ В

Филиал (Атырау)

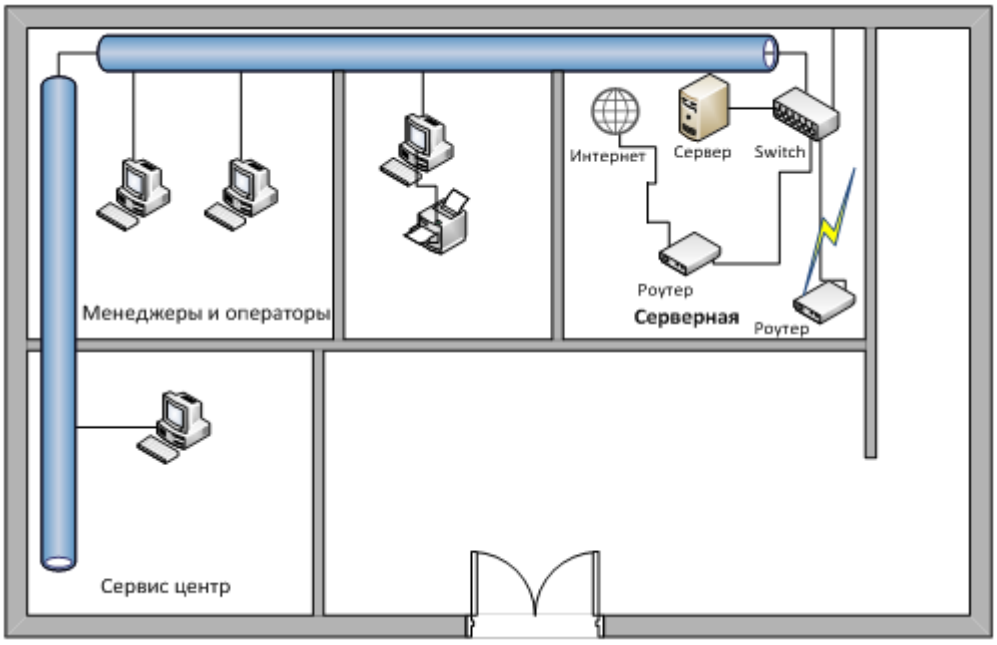

Рисунок 10 – Структура сети филиала в Атырау

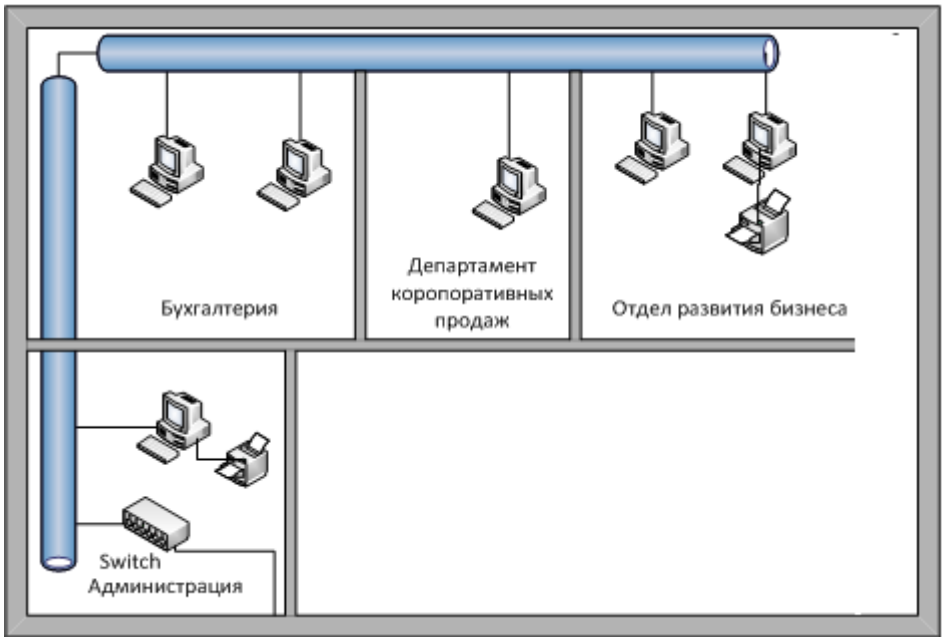

Рисунок 11 – Структура сети филиала в Атырау

ПРИЛОЖЕНИЕ Г

Расчеты длины кабеля по уровеньу Головного офиса и уровеньу филиалов (в метрах):

Секция 1									
Номер ПК	11								
Расстояние	20								
Итого	20								
Секция 2									
Номер ПК	21	22	23	24					
Расстояние	20	15	10	5					
Итого	50								
Секция 3									
Номер ПК	31	32	33	34	35				
Расстояние	20	15	10	7	5				
Итого	57								
Секция 5									
Номер ПК	51	52	53	54	55	56	57	58	
Расстояние	20	17	15	12	10	9	7	5	
Итого	95								
Секция 6									
Номер ПК	61	62	63	64	65	66	67		
Расстояние	20	17	15	12	10	9	7		
Итого	90								
Секция № 7									
Номер ПК	71	72	73	74	75				
Расстояние	20	17	15	12	10				
Итого	74								
Итого с секций	386								

Филиал 1 Секция № 1						
Номер ПК	11	12	13	14		
Расстояние	25	20	15	12		
Итого	72					
Секция № 2						
Номер ПК	21	22	23	24	25	26
Расстояние	25	20	17	15	12	10
Итого	99					
Итого с секций	171					
Общий итог	386+243*2	872				

Итого требуется 872 м кабеля на все филиалы.

Так как может погрешность в районе 2% - 3%, то следовательно будем брать около 1000 м.

131.31.0.1 (r1)

```
R1#show running-config
Building configuration...

Current configuration : 753 bytes
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R1
enable password cisco
interface FastEthernet0/0
 ip address 131.31.0.1 255.255.192.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet1/0.1
 encapsulation dot1Q 10
 ip address 131.31.64.1 255.255.192.0
!
interface Serial2/0
 no ip address
 shutdown
!
interface Serial3/0
 no ip address
 shutdown
!
interface FastEthernet4/0
 no ip address
 shutdown
!
interface FastEthernet5/0
 no ip address
 shutdown
!
router rip
 network 131.31.0.0
 network 210.10.10.0
!
ip classless
line con 0
!
line aux 0
```

```
!
line vty 0 4
 login
end
```

Switch 0

```
Switch#show running-config
Building configuration...

Current configuration : 1242 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport trunk allowed vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport trunk allowed vlan 10
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 10
 switchport trunk allowed vlan 10
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 10
!
interface FastEthernet0/6
 switchport access vlan 10!
interface FastEthernet0/5
!
interface FastEthernet0/10
 switchport mode trunk
!
line con 0
```

```
!
line vty 0 4
 login
line vty 5 15
 login
!
!
End
```

193.93.93.65 (r3)

R2#show running-config
Building configuration...

```
Current configuration : 690 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R2
!
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0

interface FastEthernet0/0
 ip address 131.31.0.2 255.255.192.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet1/0.1
 encapsulation dot1Q 20
 ip address 131.31.128.1 255.255.192.0
!
interface Serial2/0
 no ip address
 shutdown
!
interface Serial3/0
 no ip address
 shutdown
!
interface FastEthernet4/0
 no ip address
```

```
 shutdown
!
interface FastEthernet5/0
 no ip address
 shutdown
!
router rip
 network 131.31.0.0
 network 210.10.10.0
!
ip classless
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

Switch 2

```
Switch#show running-config
Building configuration...

Current configuration : 1194 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport access vlan 20
 switchport trunk allowed vlan 1,10,20,1002-1005
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 20
!
```

```
interface FastEthernet0/4
 switchport access vlan 20
!
interface FastEthernet0/5
 switchport access vlan 20
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
 switchport access vlan 20
 switchport mode access

line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end
```

193.93.93.129 (r2)

```
Router#show running-config
Building configuration...

Current configuration : 695 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
interface FastEthernet0/0
 ip address 131.31.0.3 255.255.192.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
```

```
!
interface FastEthernet1/0.1
 encapsulation dot1Q 30
 ip address 131.31.193.1 255.255.192.0
!
interface Serial2/0
 no ip address
 shutdown
!
interface Serial3/0
 no ip address
 shutdown
!
interface FastEthernet4/0
 no ip address
 shutdown
!
interface FastEthernet5/0
 no ip address
 shutdown
!
router rip
 network 131.31.0.0
 network 210.10.10.0
!
ip classless
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

switch 1

```
Switch#show running-config
Building configuration...

Current configuration : 1194 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
```

```
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport trunk allowed vlan 30
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 30
!
interface FastEthernet0/5
 switchport access vlan 30
!
interface FastEthernet0/6
 switchport access vlan 30
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
End
```

210.10.10.1 (Internet)

```
Router#show running-config
Building configuration...

Current configuration : 575 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
interface FastEthernet0/0
 ip address 210.10.10.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 ospf cost 1
```

```
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 network 131.31.0.0
 network 210.10.10.0
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```