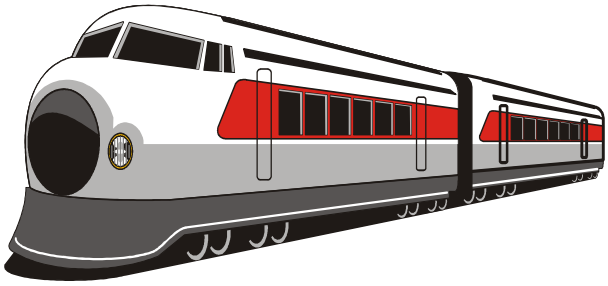
ТОШКЕНТ ТЕМИР ЙЎЛ МУҲАНДИСЛАРИ ИНСТИТУТИ



Кафедра Темир йўл транспортида ахборот тизимлари

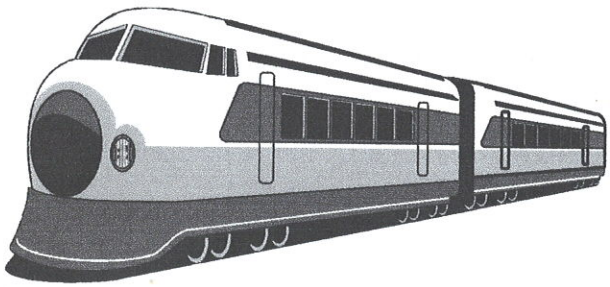
ИССЛЕДОВАНИЕ ИМИТАЦИОННОЙ МОДЕЛИ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ мавзусидаги

БИТИРУВ МАЛАКАВИЙ ИШИ

Муаллиф: Файзиев С. С.

Тошкент – 2019 й.

ТОШКЕНТ ТЕМИР ЙЎЛ МУҲАНДИСЛАРИ ИНСТИТУТИ



Ҳимоя қилишга
руҳсат берилсин
Кафедра мудири
«28» 06 2019

Кафедра «Информационные системы на железнодорожном транспорте»
Исследование имитационной модели локальных вычислительных сетей.
мавзудаги

БИТИРУВ МАЛАКАВИЙ ИШИ

Муаллиф Файзиев С. С.

Асосий маслаҳатчи Расулмухамедов М.М.

Маслаҳатчилар:
ассистент Ташметов Т.Ш.

Маслаҳатчилар Камилов Х.М.

Тақризчи Ядгаров Т.Г.

Ташкент – 2019 й.

Ш-10

Ташкентский институт инженеров железнодорожного транспорта _____
Олий ўқув юрти

«Экономика» факультети «Информационные системы на ж.д. транспорте» кафедраси

«Информатика и информационные технологии (на ж.д. транспорте)» йўналиши АТ-24 гуруҳи

Тасдиқлайман _____

Каф. мудири _____

«10» 01 2019 йил

сана

БИТИРУВ МАЛАКАВИЙ ИШИ БЎЙИЧА ТОПШИРИҚ

Талаба _____ Файзиев Сангин Собирович.

(фамилияси, исми, шарифи)

1. Битирув ишининг мавзуси «Исследование имитационной модели локальных вычислительных сетей. »

«19» декабр 2018 йил 5-сонли кафедра мажлисида маъқулланган ва институтнинг 07 январ 2019 йилги 4-Т буйруги билан тасдикланган.

2. Битирув ишини топшириш муддати _____15.06.2019_____

3.Битирув ишини бажаришга доир бошланғич маълумотлар _Локальная сеть – важный элемент любого современного предприятия, без которого невозможно добиться максимальной производительности труда.

Однако, чтобы использовать возможности сетей на полную мощность, необходимо их правильно настроить, учитывая также и то, что расположение подсоединенных компьютеров будет влиять на производительность ЛВС.

4. Ҳисоблаш-тушунтириш ёзувларининг таркиби (ишлаб чиқиладиган масалалар рўйхати) ____

1. Выбор и обоснование архитектуры сети
2.Описание существующей корпоративной вычислительной сети
3. Настройки сети на сос ubuntu server
4. Охрана труда. Опасные и вредные производственные факторы трудового процесса

5. Чизма ишлар рўйхати (чизмалар номи аниқ кўрсатилади)

1. Подключение локальной сети к сети интернет

2. Работа системы электронной почты

3. Схема реагирования

6. Битирув бўйича маслаҳатчи (лар)

№	Бўлим мавзуси	Маслаҳатчи ўқитувчи Ф.И.Ш.	Имзо, сана	
			Топшириқ берилди	Топшириқ бажарилди
1	Аналитический обзор	Ташметов Т.Ш.	01.02.2019	19.02.2019
2	Техническая часть	Ташметов Т.Ш..	20.02.2019	01.06.2019
3	Охрана труда	Камилов Х.М.	07.05.2019	06.06.2019
4	Оформление работы	Ташметов Т.Ш.	28.05.2019	15.06.2019

7. Битирув ишини бажариш режаси

№	Битирув иши босқичларининг номи	Бажариш муддати (сана)	Текширувдан ўтганлик Белгиси
1	Введение	27.01.2019	
2	1. Выбор и обоснование архитектуры сети	7.02.2019	
3	2.Описание существующей корпоративной вычислительной сети	6.03.2019	
4	3. Настройки сети на сос ubuntu server	7.04.2019	
5	Определение цели сканирования	01.06.2019	
6	Охрана труда	06.06.2019	
7	Оформление выпускной работы	15.06.2019	
8	Заключение	21.06.2019	

Битирув иши раҳбари _____ Ташметов Т.Ш. _____
(Ф.И.Ш) (имзо)

Топшириқни бажаришга олдим Файзиев С.С. _____
(Ф.И.Ш) (имзо)

Топшириқ берилган сана «_10_»_____01_____2019_ йил

Тошкент темир йўл муҳандислари институти

Факултет Информатика Кафедра Темир йўл транспортида ахб-ти

Таълим йуналиши: 5330200 «Информатика ва Ахборот технологиялари»

«Тасдиқлайман»

Каф. мудири Расулмухамедов М.

« 10 » 01 2015 йил.

Талаба Файзиев Санжар Собирович га
(фамилияси, исми, шарифи)

битирув малакавий ишини «Ҳаёт фаолияти хавфсизлиги» бўлимини бажариш бўйича

ТОПШИРИК

1.Мавзу Исследование имитационной модели беспроводных локальных сетей

кафедра кенгашининг 20___й. «__» ______________ №__ сонли баённомаси қарори билан тасдиқланган.

2.Талабанинг тугалланган бўлимни топшириш муддати________________________

3.Битирув малакавий ишини «Ҳаёт фаолияти хавфсизлиги» бўлимини бажаришга оид дастлабки маълумотлар Опасные вредные производственные факторы трудового процесса

4.Ҳисоб–тушунтириш қисмининг мазмуни (ишлаб чиқиладиган саволлар рўйхати) Правовые основы и проблемы безопасности жизнедеятельности РУз. Опасные и вредные производственные факторы трудового процесса. Методы контроля загазованности.

5.График материаллар рўйхати (аниқ номланган зарурий чизмалар)

Топшириқ олди Файзиев Санжар
(имзо, сана, талабани ф.и.ш.)

Топшириқ берди Камилов И.Н.
(сана, рахбар имзоси, лавозими, ф.и.ш.)

РЕЦЕНЗИЯ
на выпускную квалификационную работу студента Ташкентского института инженеров железнодорожного транспорта по направлению -5330200 «Информатика и информационные технологии»

Файзиев Сангин Собирович
«Исследование имитационной модели локальных вычислительных сетей.»

Актуальность темы, цель и задачи выпускной квалификационной работы обоснованы во введении. Локальная сеть – важный элемент любого современного предприятия, без которого невозможно добиться максимальной производительности труда.
Однако, чтобы использовать возможности сетей на полную мощность, необходимо их правильно настроить, учитывая также и то, что расположение подсоединенных компьютеров будет влиять на производительность Выбранная тема выпускной квалификационной работы обусловлена увеличением роли и значимости управления проектами как одного из приоритетных направлений развития по компьютерных сетей

Выпускная квалификационная работа аккуратно оформлена на компьютере, работа имеет традиционное построение: обзор литературы, иллюстрирована 19 рисунками и 10 таблицами. Все расчеты выполнены, верно и представлены в таблицах

Представленный выпускной квалификационной работы посвящен теоретически актуальной и практически важной проблеме Исследование имитационной модели локальных вычислительных сетей. Во введении обусловлена актуальность исследования, представлены основные проблемы защиты информационных системах , корректно сформулирована цель, выявлены предмет и объект исследования.

Первая глава посвящена теоретическим исследованиям информационные технологии: определение, инструментарий; информатизация Мониторинг трафика жизненно важен для эффективного управления сетью. Он является источником информации о функционировании корпоративных приложений, которая учитывается при распределении средств, планировании вычислительных мощностей, определении и локализации отказов, решении вопросов безопасности.

Во второй Выработать и реализовать сетевую политику, настроить телекоммуникационное оборудование локальной вычислительной сети образовательного учреждения. Выбрать архитектуру сети, рассчитать кабель для этой сети, подобрать оборудование и программное обеспечение.

Во третьей главе Выходные данные Nmap это список просканированных целей с дополнительной информацией по каждой в зависимости от заданных опций. Ключевой информацией является “таблица важных портов”. Эта таблица содержит номер порта, протокол, имя службы и состояние. Состояние может иметь значение open (открыт), filtered (фильтруется), closed (закрыт) или unfiltered (не фильтруется).

В четвертой главе посвящена охрана труда**.** Законы об охране труда республики Узбекистан

Действие настоящего Закона распространяется на всех работников, состоящих в трудовых отношениях с предприятиями, учреждениями, организациями различных форм собственности и хозяйствования, в том числе с отдельными нанимателями; членов кооперативов, студентов высших учебных заведений, учащихся средних специальных учебных заведений, профессионально-технических училищ и общеобразовательных школ, проходящих производственную практику; военнослужащих, привлекаемых для работы на предприятиях.

Предложенные в выпускной квалификационной работе мероприятия и предложения по совершенствованию системы управления проектами в организации являются новыми для организации и практически значимыми.

В работе выявлены незначительные орфографические и стилистические ошибки. Также есть неточности в списке литературы и некоторых ссылках.

Задание на выпускную квалификационную работу выполнено полностью. На основании представленных материалов считаю, что работа заслуживает оценки «отлично».

Рецензент_____ Ядгаров Т.Г.
(Подпись) (Ф.И.О.)

к.ф.-м.н. сб.науч.сотр., доцент.
(ученая степень, знание, должность, место работы)
ТАТУ "Олий математика"

«__»_____2019г.
(дата выдачи)

ОТЗЫВ

руководителя на выпускную квалификационную работу студента Ташкентского института инженеров железнодорожного транспорта по направлению -5330200 «Информатика и информационные технологии»

Файзиев Сангин Собирович
(Ф.И.О. слушателя)

выполненную на тему: Исследование имитационной модели локальных вычислительных сетей.

1.Актуальность, новизна:

Актуальность темы, цель и задачи выпускной квалификационной работы обоснованы во введении.

Актуальность выбранной темы обусловлена современный этап развития компьютерных сетей, использование вычислительных сетей даёт предприятию многочисленные возможности. Конечной целью использования вычислительных сетей на предприятии является повышение эффективности его работы, которое может выражаться, например, в увеличении прибыли предприятия.

2. Достоинства работы:

Выпускная квалификационная работа имеет традиционное построение: обзор литературы, подготовленный по 13 источникам учебной и периодической литературы.

Необходимо отметить тщательность анализа всех источников информации.

Выпускная квалификационная работа аккуратно оформлена на компьютере, иллюстрирована 17 рисунками. Все расчеты выполнены верно и представлены в таблицах.

3. Практическая значимость работы и рекомендации по внедрению:

Предложенные в выпускной квалификационной работе мероприятия и предложения по совершенствованию системы управления проектами в организации являются новыми для организации и практически значимыми.

4. Дополнительная информация для ГАК:

За время выполнения выпускной квалификационной работы автор продемонстрировал способность не только самостоятельно решать поставленную задачу, но и творчески подходить к самой ее постановке и предлагать новые решения.

Задание на выпускную квалификационную работу выполнено полностью.

Выпускная квалификационная работа по своему содержанию и объему отвечает установленным требованиям, может быть допущена к защите и оценивается на «отлично».

Руководитель _____ __Ташметов Т.Ш. ____
(Подпись) (Ф.И.О.)

_____ассистент _____
(ученая степень, знание, должность, место работы)

«20» июня 2019 г.
(дата выдачи)

Оглавление

ВВЕДЕНИЕ

3 апреля 2019 года Президент Шавкат Мирзиёев провел совещание, на котором были обсуждены методы практической реализации пяти инициатив, создания условий для воспитания и образования молодежи, повышения занятости женщин. Из пяти инициативах, третья инициатива – эффективное использование компьютерных технологий и интернета, для чего до 2020 года в республике будут созданы бесплатные учебные центры по цифровым технологиям и около 19 тысяч объектов социальной сферы будут обеспечены высокоскоростным доступом в интернет [1].

В этой выпускной работе предстоит: выработать и реализовать сетевую политику, настроить телекоммуникационное оборудование локальной вычислительной сети образовательного учреждения. Выбрать архитектуру сети, рассчитать кабель для этой сети, подобрать оборудование и программное обеспечение. Работы по созданию ЛВС начались еще в 60-х годах с попытки внести новую технологию в телефонную связь. Эти работы не имели серьезных результатов вследствие дороговизны и низкой надежности электроники. В начале 70-х годов в исследовательском центре компании "Xerox", лабораториях при Кембриджском университете и ряде других организаций было предложено использовать единую цифровую сеть для связи мини-ЭВМ. Использовалась шинная и кольцевая магистрали, данные передавались пакетами со скоростью более 2 Мбит/с.В конце 70-х годов появились первые коммерческие реализации ЛВС: компания "Prime" представила ЛВС "RingNet", компания "Datapoint" - ЛВС "Attached Resourse Computer" (ARC) с высокоскоростным коаксиальным кабелем. В 1980 году в институте инженеров по электротехнике и электронике IEEE (Institute of Electrical and Electronic Engeneers) организован комитет "802" по стандартизации ЛВС. В дальнейшем темпы развития ускорились, и на сегодняшний день имеется большое количество коммерческих реализаций

ЛВС. Локальная вычислительная сеть Local Area Network, LAN — компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий. Также существуют локальные сети, узлы которых разнесены географически на расстояния более 12 500 км. Несмотря на такие расстояния, подобные сети всё равно относят к локальным. Существует множество способов классификации сетей. Основным критерием классификации принято считать способ администрирования. То есть в зависимости от того, как организована сеть и как она управляется, её можно отнести к локальной, распределённой, городской или глобальной сети. Управляет сетью или её сегментом сетевой администратор. В случае сложных сетей их права и обязанности строго распределены, ведётся документация и журналирование действий команды администраторов. Компьютеры могут соединяться между собой, используя различные среды доступа: медные проводники , оптические проводники и через радиоканал. Проводные, оптические связи устанавливаются через Ethernet, беспроводные — через Wi-Fi, Bluetooth, GPRS и прочие средства. Отдельная локальная вычислительная сеть может иметь связь с другими локальными сетями через шлюзы, а также быть частью глобальной вычислительной сети или иметь подключение к ней. Чаще всего локальные сети построены на технологиях Ethernet или Wi-Fi. Следует отметить, что ранее использовались протоколы Frame Relay, Token ring, которые на сегодняшний день встречаются всё реже, их можно увидеть лишь в специализированных лабораториях, учебных заведениях и службах.

1. ВЫБОР И ОБОСНОВАНИЕ АРХИТЕКТУРЫ СЕТИ

Клиент-сервер — сетевая архитектура, в которой устройства являются либо клиентами, либо серверами. Клиентом является запрашивающая машина обычно ПК, но так же в качестве клиента могут выступать такие устройства как: сетевой принтер или прочие устройства, сервером — машина, которая отвечает на запрос. Оба термина могут применяться как к физическим устройствам, так и к программному обеспечению. Сеть с выделенным сервером — это локальная вычислительная сеть LAN, в которой сетевые устройства централизованы и управляются одним или несколькими серверами. Индивидуальные рабочие станции или клиенты такие, как ПК должны обращаться к ресурсам сети через сервер. Локальная сеть образовательного учреждения не предполагает наличия сложной иерархической структуры. Как правило, для управления сетью достаточно одного сервера. Конфигурация сервера может содержать следующие сервисы, такие как :

- Файл сервер
- Автоматическое конфигурирование рабочих станций DHCP
- Сервер имен DNS
- Локальный почтовый сервер
- Сервер печати
- Сервер кеширования Web данных из интернет Proxy server
- Сервер баз данных SQL

Сеть фактически состоит из одной рабочей группы. При количестве рабочих мест менее 10 в нашем случае 13 и в случае, если бы совместный доступ к Интернет не требовался , можно бы было обойтись без сервера только одноранговой сетью одноранговая сеть. Это бы позволило уменьшить затраты, но, вместе с тем, существенно снизит возможности сети и информационную безопасность.

Пример сети с выделенным сервером на базе СОС Ubuntu Server. Распределение ресурсов, таких как : совместный доступ к данным, общие принтеры, другие совместно используемые периферийные устройства, организуется путем предоставления локальных ресурсов и периферийных устройств в общее пользование, хотя не исключено и использование сетевых устройств, главным образом принтеров. Сервер, помимо основной задачи, - хранения данных, может являться также и сервером приложений. Например обеспечивать совместный доступ к базе данных, подключения к Интернет и т.д. Как правило сеть не требует постоянного администрирования. Для поддержания сети в рабочем состоянии достаточно еженедельного проведения профилактических работ.

1.1 Масштабируемость

Масштабируемость — в электронике и информатике означает способность системы, сети или процесса справляться с увеличением рабочей нагрузки при добавлении ресурсов. Масштабируемость — важный аспект электронных систем, систем баз данных, маршрутизаторов, если для них требуется возможность работать под большой нагрузкой. Система называется масштабируемой, если она способна увеличивать производительность пропорционально дополнительным ресурсам. Масштабируемость можно оценить через отношение прироста производительности системы к приросту используемых ресурсов. Чем ближе это отношение к единице, тем лучше. Требования к масштабируемости (общие планы на развитие, план финансирования в следующем периоде - таблица, рост потребностей в будущем - таблица). Данное заведение планирует увеличить кол-во кабинетов оснащенных вычислительной техникой на 1 - 2 компьютеров в каждом кабинете в течение 1 года. Учебное заведение планирует расширить пропускную способность интернет канала до 10 мбит в течение 2-х лет. Учебное заведение планирует открыть 1 свои филиал (5 компьютеров) в том же городе в течении 2-х лет с

аналогичной организационной структурой. Данное заведение планирует создать 1 дополнительных структурных подразделений (8 компьютеров).

1.2. Обзор существующих решений

Продукты для моделирования работы сети значительно отличаются друг от друга по цене, сложности и функциональным возможностям. Например, в этом секторе рынка можно встретить цены от 129 до 40 000 дол. и больше (если принять во внимание стоимость дополнительных модулей). Однако, ни один из продуктов нельзя рассматривать как полностью готовое к употреблению средство, способное в точности смоделировать работу существующей или даже вновь спроектированной сети. Необходимо потратить значительные средства на обучение, прежде чем станут возможными построение корректных моделей и интерпретация полученных результатов. Затем понадобится еще в течение шести-девяти месяцев непрерывно подстраивать модель, и только после этого она будет хотя бы приблизительно приведена в соответствие с действительностью.

Чтобы понять, почему так получается, надо вспомнить, как строятся модели при работе с этими продуктами. Все программы оснащены средствами графического проектирования, позволяющими строить схемы сети с помощью буксировки значков, соответствующих различным устройствам, из библиотеки на рабочее поле программы. Далее указывается, каким образом устройства соединены LAN- и WAN-каналами, работающими на разных скоростях, и, наконец, схема дополняется данными о работе сети, полученными от сетевых мониторов.

Получив все эти данные, программа строит систему математических уравнений, с помощью которых моделируется поведение сети. К сожалению, одна-две ошибки в начальной информации могут испортить все.

Каждый из рассмотренных продуктов имеет свою собственную "экологическую" нишу. Одни средства рассчитаны на управление

локальными сетями, а другие предназначены для администраторов территориально-распределенных сетей. Одни просто позволяют строить схемы сетей и обладают ограниченными возможностями моделирования, другие же способны производить сложный анализ глобальных сетей.

Однако ни одно из средств не способно охватить все задачи, поэтому если необходимо смоделировать сеть и проанализировать ее работу, придется покупать несколько продуктов. Имеются также заметные различия между продуктами, которые, как утверждается, решают одни и те же задачи.

Следует обязательно выяснить, работу каких сетевых элементов способно рассчитывать то или иное средство. В этой области можно найти интересные результаты. Большинство продуктов рассчитывают, как будут работать те элементы сети, о которых у них имеются данные. Однако три пакета сплоховали: CANE от Image Net не может моделировать работу дисков, микросхем и контроллеров; Virtual Agent от Network Tools не принимает во внимание работу с очередями и скорость передачи данных по физическому носителю; SimuNet от Telenix не в состоянии учитывать, например, архитектуру устройств. За исключением NetArchitect от Datametrics, ни одно средство не умеет смоделировать работу системы в целом. Это означает, что невозможно принять во внимание, например, влияние параметров конечных станций. По-видимому, к этой проблеме производители обратятся несколько позже, когда станут более распространенными сети, при построении которых учитывается характер работающих в них приложений. Службы каталогов и сетевые протоколы в таких сетях будут поддерживать передачу трафика, чувствительного к задержкам.

Кроме того, средства моделирования сетей имеют несколько ограниченные возможности учета воздействия на пропускную способность сети работы с приоритетами и уровнями обслуживания. Если вспомнить, какое значение сейчас придается средствам предоставления уровней обслуживания и управления ими, станет ясно, что этот недостаток должен

быть исправлен. Еще один важный момент - передача голоса через IP. Ясно, что производители средств моделирования будут обращать все больше внимания на эту проблему, по мере того как компании, стремящиеся переложить свой междугородний телефонный трафик на Internet, будут пытаться оценить воздействие соответствующей нагрузки на свои сети, базирующиеся на маршрутизаторах. Можно также ожидать появления новых компаний, которые сосредоточат свои усилия на новых технологиях, таких как Gigabit Ethernet и IP-телефония.

Таблица 1 - Услуги Интернет

№	Характеристика	Значение
1	Тип соединения с провайдером	По коммутируемой линии/ по выделенной линии
2	Среда передачи (для выделенной линии)	Медный кабель, оптоволоконная линия связи, радиоканал, спутниковый канал
3	Диапазон выделяемых IP адресов	196.34.19.2 - 196.34.19.254
4	Маска сети для выделяемых IP адресов	255.255.255.0
5	Адрес шлюза провайдера	196.34.19.1
6	Адрес DNS сервера провайдера	192.68.12.254

Таблица 2 - Трафик

Сервис	Провайдер	Цена	Количество
Абонентская плата	Домолинк	340/ месяц	Неограниченно

1.3 Основные задачи оптимизации локальных сетей

Для того, чтобы сеть работала самым эффективным образом, необходимо решить следующие задачи:

1. С формулировать критерии эффективности работы сети. Чаще всего такими критериями служат производительность и надежность, для которых в свою очередь требуется выбрать конкретные показатели оценки, например, время реакции и коэффициент готовности, соответственно.

2. Определить множество варьируемых параметров сети, прямо или косвенно влияющих на критерии эффективности. Эти параметры действительно должны быть варьируемыми, то есть нужно убедиться в том, что их можно изменять в некоторых пределах. Так, если размер пакета какого-либо протокола в конкретной операционной системе устанавливается автоматически и не может быть изменен путем настройки, то этот параметр в данном случае не является варьируемым, хотя в другой операционной системе он может относится к изменяемым по желанию администратора, а значит и варьируемым. Другим примером может служить пропускная способность внутренней шины маршрутизатора – она может рассматриваться как параметр оптимизации только в том случае, если допускается возможность замены маршрутизаторов в сети.

Все варьируемые параметры могут быть сгруппированы различным образом. Например, параметры отдельных конкретных протоколов (максимальный размер кадра протокола Ethernet или размер окна неподтвержденных пакетов протокола TCP) или параметры устройств (размер адресной таблицы или скорость фильтрации моста, пропускная способность внутренней шины маршрутизатора). Параметрами настройки могут быть и устройства, и протоколы в целом. Так, например, улучшить работу сети с медленными и зашумленными глобальными каналами связи можно, перейдя со стека протоколов IPX/SPX на протоколы TCP/IP. Также можно добиться значительных улучшений с помощью замены сетевых адаптеров неизвестного производителя на адаптеры BrandName.

3. Определить порог чувствительности для значений критерия эффективности. Так, производительность сети можно оценивать логическими значениями "Работает"/"Не работает", и тогда оптимизация сводится к диагностике неисправностей и приведению сети в любое работоспособное состояние. Другим крайним случаем является тонкая настройка сети, при которой параметры работающей сети (например, размер кадра или величина окна неподтвержденных пакетов) могут варьироваться с целью повышения

производительности (например, среднего значения времени реакции) хотя бы на несколько процентов. Как правило, под оптимизацией сети понимают некоторый промежуточный вариант, при котором требуется выбрать такие значения параметров сети, чтобы показатели ее эффективности существенно улучшились, например, пользователи получали ответы на свои запросы к серверу баз данных не за 10 секунд, а за 3 секунды, а передача файла на удаленный компьютер выполнялась не за 2 минуты, а за 30 секунд.

Таким образом, можно предложить три различных трактовки задачи оптимизации:

1. Приведение сети в любое работоспособное состояние. Обычно эта задача решается первой, и включает:

- поиск неисправных элементов сети – кабелей, разъемов, адаптеров, компьютеров;
- проверку совместимости оборудования и программного обеспечения;
- выбор корректных значений ключевых параметров программ и устройств, обеспечивающих прохождение сообщений между всеми узлами сети – адресов сетей и узлов, используемых протоколов, типов кадров Ethernet и т.п.

2. Грубая настройка – выбор параметров, резко влияющих на характеристики (надежность, производительность) сети. Если сеть работоспособна, но обмен данными происходит очень медленно (время ожидания составляет десятки секунд или минуты) или же сеанс связи часто разрывается без видимых причин, то работоспособной такую сеть можно назвать только условно, и она нуждается в грубой настройке. На этом этапе необходимо найти ключевые причины существенных задержек прохождения пакетов в сети. Обычно причина серьезного замедления или неустойчивой работы сети кроется в одном неверно работающем элементе или некорректно установленном параметре, но из-за большого количества возможных виновников поиск может потребовать длительного наблюдения за работой сети и громоздкого перебора вариантов. Грубая настройка во многом похожа

на приведение сети в работоспособное состояние. Здесь также обычно задается некоторое пороговое значение показателя эффективности и требуется найти такой вариант сети, у которого это значение было бы не хуже порогового. Например, нужно настроить сеть так, чтобы время реакции сервера на запрос пользователя не превышало 5 секунд.

3. Тонкая настройка параметров сети (собственно оптимизация). Если сеть работает удовлетворительно, то дальнейшее повышение ее производительности или надежности вряд ли можно достичь изменением только какого-либо одного параметра, как это было в случае полностью неработоспособной сети или же в случае ее грубой настройки. В случае нормально работающей сети дальнейшее повышение ее качества обычно требует нахождения некоторого удачного сочетания значений большого количества параметров, поэтому этот процесс и получил название "тонкой настройки".

Даже при тонкой настройке сети оптимальное сочетание ее параметров получить невозможно, да и не нужно. Нет смысла затрачивать колоссальные усилия по нахождению строгого оптимума, отличающегося от близких к нему режимов работы на величины такого же порядка, что и точность измерений трафика в сети. Достаточно найти любое из близких к оптимальному решений, чтобы считать задачу оптимизации сети решенной. Такие близкие к оптимальному решения обычно называют рациональными вариантами, и именно их поиск интересует на практике администратора сети или сетевого интегратора.

Поиск неисправностей в сети – это сочетание анализа (измерения, диагностика и локализация ошибок) и синтеза (принятие решения о том, какие изменения надо внести в работу сети, чтобы исправить ее работу).

- Анализ – определение значения критерия эффективности (или, что одно и то же, критерия оптимизации) системы для данного сочетания параметров сети. Иногда из этого этапа выделяют подэтап мониторинга, на котором выполняется более простая процедура – процедура сбора первичных

данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов и т.п. Далее выполняется этап собственно анализа, под которым в этом случае понимается более сложный и интеллектуальный процесс осмысления собранной на этапе мониторинга информации, сопоставления ее с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадежной работы сети. Задача мониторинга решается программными и аппаратными измерителями, тестерами, сетевыми анализаторами и встроенными средствами мониторинга систем управления сетями и системами. Задача анализа требует более активного участия человека, а также использования таких сложных средств как экспертные системы, аккумулирующие практический опыт многих сетевых специалистов.

1.4. Базовые структуры современных сетей предприятия

Транспортная система локальных сетей масштаба здания или кампуса уже достаточно давно стала включать разнообразные типы активного коммуникационного оборудования - повторители, концентраторы, коммутаторы и маршрутизаторы, соединенные в сложные иерархические структуры

Описанный подход стал нормой при проектировании крупных сетей и полностью вытеснил сети, построенные исключительно на основе пассивных сегментов кабеля, которыми совместно пользуются для передачи информации компьютеры сети. Преимущества сетей с иерархически соединенным активным оборудованием не раз проверены на практике и сейчас никем не оспариваются.

Если не обращать внимание на типы используемого оборудования, а рассматривать их просто как много портовые черные ящики, то может сложиться впечатление, что никаких других изменений в теории и практике

построения локальных сетей нет - предлагаются и реализуются очень похожие схемы, отличающиеся только количеством узлов и уровней иерархии коммуникационного оборудования.

Однако, качественный анализ используемого оборудования говорит об обратном. Изменения есть, и они существенны. За последние год-два коммутаторы стали заметно теснить другие виды активного оборудования с казалось бы прочно завоеванных позиций. Несколько лет назад в типичной сети здания нижний уровень иерархии всегда занимали повторители и концентраторы, верхний строился с использованием маршрутизаторов, а коммутаторам отводилось место где-то посередине, на уровне сети этажа. К тому же, коммутаторов обычно было немного - их ставили только в очень загруженные сегменты сети или же для подключения сверхпроизводительных серверов.

Коммутаторы стали вытеснять маршрутизаторы из центра сети на периферию, где они использовались для соединения локальной сети с глобальными.

Центральное место в сети здания занял модульный корпоративный коммутатор, который объединял на своей внутренней, как правило, очень производительной, магистрали все сети этажей и отделов. Коммутаторы потеснили маршрутизаторы потому, что их показатель "цена/производительность", рассчитанный для одного порта, оказался гораздо ниже при приближающихся к маршрутизаторам функциональным возможностям по активному воздействию на передаваемый трафик. Сегодняшние корпоративные коммутаторы умеют многое из того, что несколько лет назад казалось исключительной прерогативой маршрутизаторов: транслировать кадры разных технологий локальных сетей, например Ethernet в FDDI, осуществлять фильтрацию трафика по различным условиям, в том числе и задаваемым пользователем, изолировать трафик одного сегмента от другого и т.п. Коммутаторы ввели также и новую технологию, которая до их появления не применялась -

технологию виртуальных сегментов, позволяющих перемещать пользователей из одного сегмента в другой чисто программным путем, без физической пере коммутации разъемов. И при всем при этом стоимость за один порт при равной производительности у коммутаторов оказывается в несколько раз ниже, чем у маршрутизаторов.

После завоевания магистрального уровня корпоративной сети коммутаторы начали наступление на сети рабочих групп, где до этого в течение последних пяти лет всегда использовались многопортовые повторители (концентраторы) для витой пары, заменившие пассивные коаксиальные сегменты. Появились коммутаторы, специально предназначенные для этой цели - простые, часто неуправляемые устройства, способные только быстро передавать кадры с порта на порт по адресу назначения, но не поддерживающие всей многофункциональности корпоративных коммутаторов. Стоимость таких коммутаторов в расчете на один порт быстро снижается и, хотя порт концентратора по-прежнему стоит меньше порта коммутатора рабочей группы, тенденция к сближению их цен налицо.

Типичная структура сети масштаба предприятия в общем виде приведена в таблица.3.

При всем разнообразии структурных схем сетей, построенных на коммутаторах, все они используют две базовые структуры - стянутую в точку магистраль и распределенную магистраль. На основе этих базовых структур затем строятся разнообразные структуры конкретных сетей

Стянутая в точку магистраль (collapsed backbone) - это структура, при которой объединение узлов, сегментов или сетей происходит на внутренней магистрали коммутатора. Пример сети рабочей группы, использующей такую структуру, приведен на рис 1.

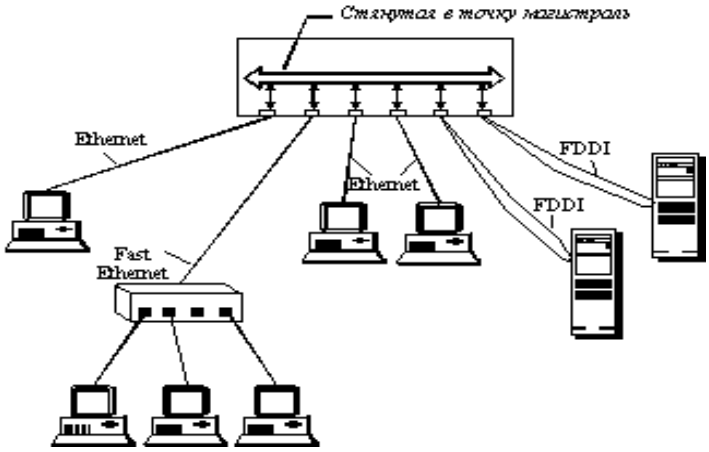


Рис. 1 Стянутая в точку магистраль на коммутатор

Таблица 3 - Оборудование

Маршрутизатор CISCO1802W-AG-E/K9	ADSL/ISDN with 802.11a+g ETSI Compliant and Security
Свич CATALIST 3560 24 PoE + 4 SFP	24 порта, UTP 5, настольное исполнение.
Хабы	Office Connect Ethernet Hub 3C16702A/TP16C 16 port RJ-45+ 1 port BNC

Таблица 4 - Поставщики оборудования

Никс	www.nix.ru	Рабочие станции, сервер
Ромбо	www.rombo.ru	Компьютерная техника
ITEL LTD	www.itel.com.ua	Сетевое оборудование

Проект ЛВС здания

Определить места расположения активного и пассивного оборудования, рекомендации по расположению классов, кроссировку кабельной сети.

Таблица 5 - Проект ЛВС

Оборудование	Комната
Маршрутизатор	104 (серверная)
Сервер	104 (серверная)
Свитч	104 (серверная)
Хабы	101,102,103,104,105,106,107

Таблица 7 - Топология, среда передачи

Звезда	Медные провода - витая пара /UTP Level 5/	
Подключение к Интернет	Точка-точка	Выделенная линия (ISDN)
Подключение филиалов	Точка-точка	Коммутируемая линия

При топологии «звезда» показ (рис 2.) все компьютеры с помощью сегментов кабеля подключаются к центральному компоненту, именуемому концентратором. Сигналы от передающего компьютера поступают через концентратор ко всем остальным. Эта топология возникла на заре вычислительной техники, когда компьютеры были подключены к центральному, главному, компьютеру.

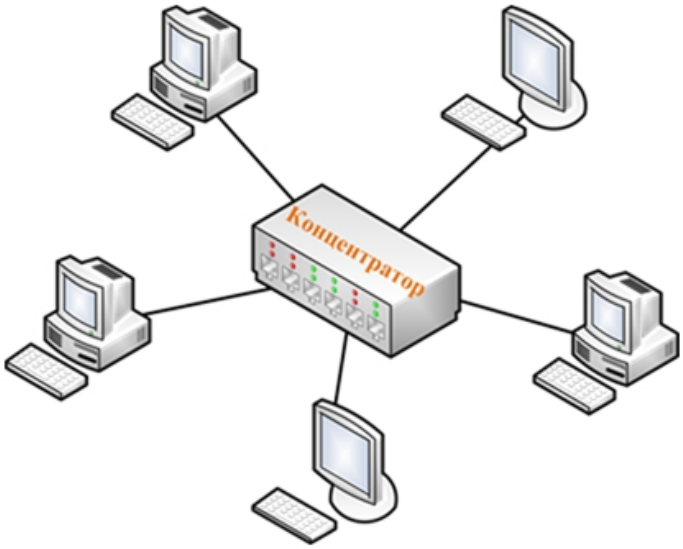


Рис 2 .Сеть с топологией «звезда"

В сетях с топологией «звезда» подключение кабеля и управление конфигурацией сети централизованы. Но есть и недостаток: так как все компьютеры подключены к центральной точке, для больших сетей значительно увеличивается расход кабеля. К тому же, если центральный компонент выйдет из строя, нарушится работа всей сети.

2. ОПИСАНИЕ СУЩЕСТВУЮЩЕЙ КОРПОРАТИВНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

2.1. Обзор сетевых кабелей

На схеме расположено 14 ПК, 3 коммутатора, 1 маршрутизатор и 14 IP - телефонов. К первому коммутатору подключены ПК и IP-телефоны директора (VLAN2) и главного бухгалтера(VLAN 3). Ко второму коммутатору подключены ПК и IP-телефоны персонала (VLAN4) данной компании (6 штатных менеджеров, бухгалтер, кассир, секретарь, а также входит ПК, расположенный в конференц-зале). К третьему коммутатору подключенs ПК и IP-телефоны системного администратора (VLAN11) и охранника (VLAN5) . Коммутаторы соединены между собой .

К первому коммутатору также подключен роутер, через который каждый сотрудник имеет доступ в сеть Internet и Wi-Fi модуль для беспроводного соединения клиентов и сотрудников.

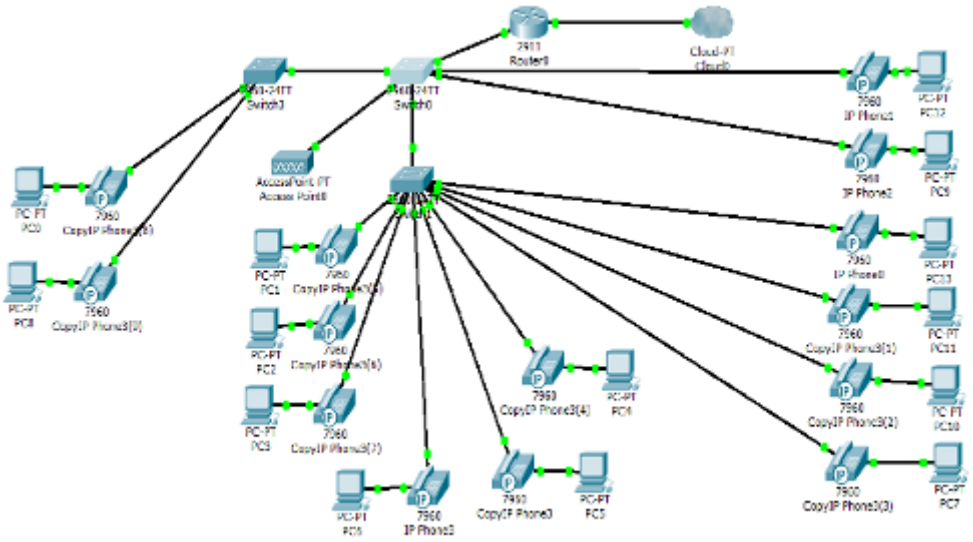


Рис 3- Логическая схема аудиторий.

Для локальных сетей существует три принципиальные схемы соединения: с помощью витой пары, коаксиального или волоконно-оптического кабеля. Для передачи информации так же могут использоваться

спутники, лазеры, микроволновое излучение и т.п., но подобное оборудованиее выходит за область рассмотрения этого курсового проекта.

Витая пара в настоящее время является самой распространённой средой передачи и представляет собой пару свитых проводов. Кабель, составленный из нескольких витых пар, как правило, покрыт жёсткой пластиковой оболочкой, предохраняющей его от воздействия внешней среды и механических повреждений.

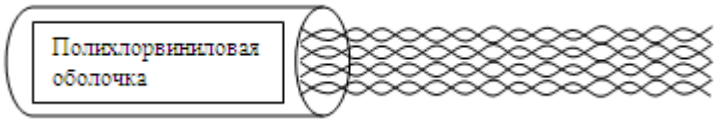


Рис 4 - Кабель из витых пар

В нормальных условиях витая пара поддерживает скорость передачи данных до 100 Мбит/с. Однако ряд факторов может существенно снизить скорость передачи данных, в частности, потеря данных, перекрёстное соединение и влияние электромагнитного излучения.

Для уменьшения влияния электрических и магнитных полей применяется экранирование. Но после экранирования витой пары в значительной степени увеличивается затухание сигнала. Под затуханием сигнала подразумевается его ослабление при передаче из одной точки сети в другую. Экранирование изменяет сопротивление, индуктивность и ёмкость таким образом, что линия становится склонной к потере данных.

Кабель пятой категории является самой распространённой средой передачи для Ethernet. Кабель поддерживает скорость передачи данных до 100Мбит/с и используется в сетях с архитектурой 100base-T и 10base-T. Кабель тактируется частотой 100 МГц.

Устройство волоконно-оптического кабеля

Коаксиальный и волоконно-оптический кабель устроены почти одинаково. Сердечник последнего состоит из сплетения тонких стеклянных волокон и заключён в пластиковую оболочку, отражающую свет обратно к

сердечнику. Плакирование покрыто концентрическим защитным слоем пластика. На рис.7 показано устройство волоконно-оптического кабеля.

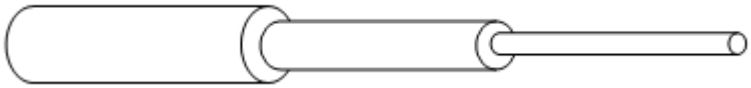


Рис 5 - Волоконно-оптический кабель

Все данные в компьютере представляются с помощью нулей и единиц. Все стандартные кабели передают бинарные данные с помощью электрических импульсов. И только волоконно-оптический кабель, используя тот же принцип, передаёт данные с помощью световых импульсов. Источник света посылает данные по волоконно-оптическому «каналу», а принимающая сторона должна преобразовать полученные данные в необходимый формат.

Одномодовый и многомодовый кабель

В относительно тонком волоконно-оптическом канале свет будет распространяться вдоль продольной оси канала. В учебниках физики этот эффект упоминается в следующей формулировке – «импульсы света распространяются в осевом (аксиальном) направлении». Именно это и происходит в одномодовом кабеле.

Однако преимущества этого типа передачи ограничены. С целью устранения подобных ограничений стали выпускать подобный кабель. Но тут возникла другая проблема – лучи света имеют свойство входить в канал под различными углами волны проходят различное расстояние и прибывают к получателю в разное время. Этот эффект, получил название модальной дисперсии, по этому кабелю подается интернет до здания и для согласования оптоволокна и витой пары применяют медиаконвертер.

Источник света Волоконно-оптический кабель Приёмник 1

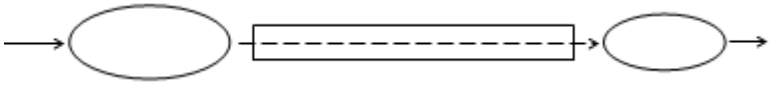


Рис 6 - Принцип работы волоконно-оптического кабеля.

Оболочка Плакирование

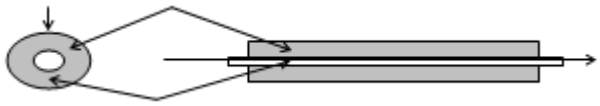


Рис 7 - Свет распространяется по одномодовому пути

Оболочка Плакирование Аксиальный луч

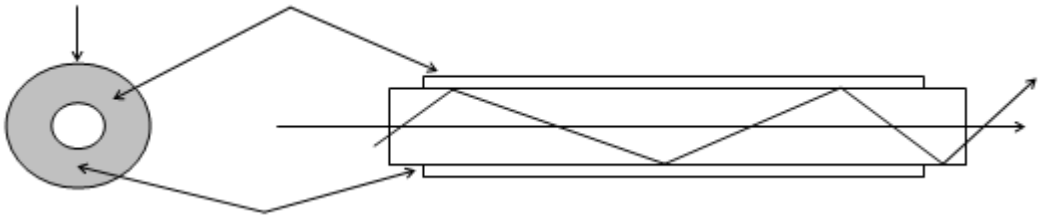


Рис 8 -Лучи подвержены модальной дисперсии

Чем больше количество мод света в канале, тем уже полоса пропускания. В дополнение к тому, что различные импульсы достигают получателя практически одновременно, усиление дисперсии приводит к наложению импульсов и введению получателя в «заблуждение». В результате снижается общая пропускная способность. Одномодовый кабель передаёт только одну моду световых импульсов. Скорость передачи данных при этом достигает десятков гигабит в секунду. Одномодовый кабель в состоянии поддерживать несколько гигабитных каналов одновременно, используя для этого световые волны разной длины. Следовательно, пропускная способность многомодового волоконно-оптического кабеля ниже, чем у одномодового.

Простейший способ уменьшения дисперсии – нивелирование волоконно-оптического кабеля. В результате лучи света синхронизируются таким образом, что дисперсия на стороне приёмника уменьшается. Дисперсия также может быть уменьшена путем ограничения количества

длин световых волн. Оба метода позволяют в некоторой степени уменьшить дисперсию, но не в состоянии привести скорость передачи данных в соответствие с одномодовым волоконно-оптическим кабелем.

В США широко используется многомодовый волоконно-оптический кабель 62.5/125. Обозначение «62.5» соответствует диаметру сердечника, а обозначение «125» – диаметру плакирования (все величины приведены в микронах). Из одномодовых распространены кабели с маркировкой 5-10/125. Ширина полосы пропускания обычно приводится в МГц/км. Хорошей моделью взаимоотношений полосы пропускания и дальности передачи служит резиновый жгут – с увеличением расстояния полоса пропускания сужается (и наоборот). В случае передачи данных на расстояние 100 метров полоса частот многомодового кабеля составляет 1600 Мгц при длине волны 850 нм. Аналогичная характеристика одномодового кабеля составляет приблизительно 888 ГГц.

Основные характеристики волоконно-оптического кабеля:

Абсолютный иммунитет к электромагнитным излучениям.

Возможна передача данных на расстояние до 10 км.

В лабораторных условиях реально достичь скорости передачи до 4 Гбит/с.

В качестве источника света может использоваться светоизлучающий диод или лазер.

2.2. Расчет количества кабеля и кабель-канала

На каждом рабочем месте устанавливается внешняя компьютерная розетка. Всего устанавливается 28 розеток. К каждой розетке прокладывается кабель «неэкранированная витая пара» (UTP). Соединение горизонтальной проводки с портами активного сетевого оборудования осуществляется коммутационными шнурами длиной один метр. Для подключения рабочих станций к розеткам используются коммутационные шнуры длиной 1 метр. Количество данных шнуров равно 14. Прокладка кабеля выполняется по периметру помещения в кабель-каналах. Кабель прокладывается на высоте

не менее 0,5 м от пола. Общая длина кабеля будет равна сумме длин кабеля от каждой розетки до шкафа. Всего нам понадобиться 120м кабеля.

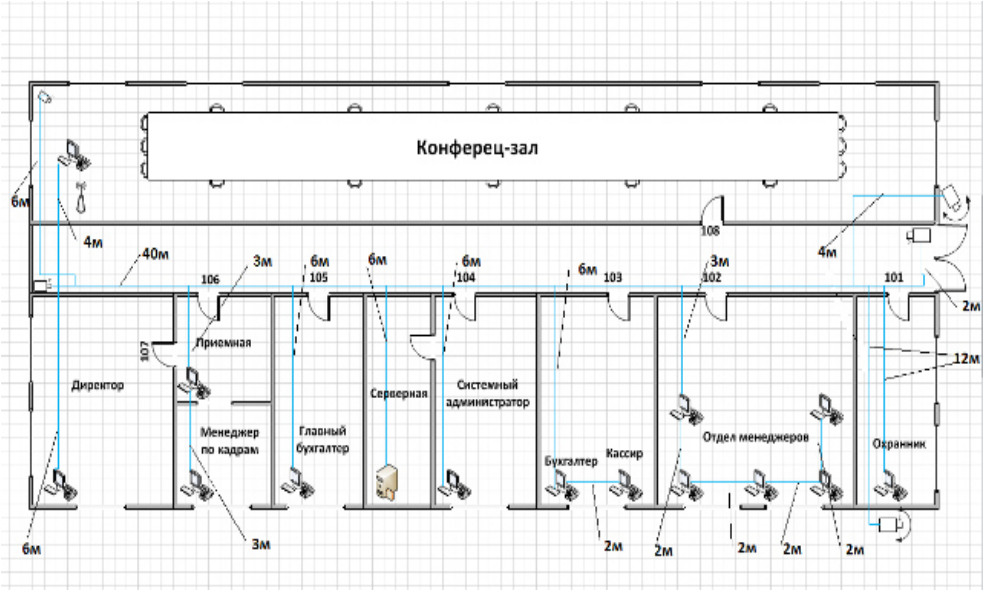


Рис 9 - Расчет кабеля

Вдоль всего хола протягиваем лоток. Из кабинета 107 протягиваем кабель от ПК директора вдоль стены и подключаем его к лотку .Из кабинета 106 протягиваем кабель вдоль стены от обоих ПК к лотку. Из кабинета 105 вдоль стены протягиваем кабель от ПК главного бухгалтера и подключаем его к лотку.

Из серверной протягиваем кабель вдоль стены, сверлим отверстие и подключаем к лотку. Из 104 кабинета протягиваем кабель от ПК системного администратора и подключаем его к лотку. Кабинет 103 содержит также 2 ПК : 1, 2. ПК1 – головной, поэтому соединяем его с ПК2 и протягиваем кабель вдоль стены к лотку. Кабинет 105 содержит 5 ПК : 1, 2, 3, 4, 5. ПК1 – головной, следовательно протягиваем от него кабель к лотку и соединяем все 5 ПК между собой. Через кабинет 101 от лотка вдоль стены протягиваем кабель, сверлим отверстие на улицу и подключаем видеокамеру, здесь же , от ПК охранника вдоль стены протягиваем еще один кабель к лотку. Возле главного входа устанавливаем видеокамеру , ведем кабель над главным входом к лотку. В кабинете 108 сверлим отверстие на улицу , подключаем

видеокамеру, смотрящую на главный вход и ведем от нее кабель также над главным входом (в помещении) к лотку.

Так же из кабинета 108 протягиваем вдоль стены кабель от ПК к лотку. В кабинете 108 устанавливаем видеокамеру и также протягиваем кабель к лотку.

Таблица 11 - Расчет кабеля

Кабинет	Кабель,м.
Хол	40м
107	6м
Главный вход	2м
101	12м
102	11м
103	8м
104+Серверная	12м
105	6м
106	6м
108+Хол	18м

В сетях больших зданий или кампусов использование структуры с классированной магистралью не всегда рационально или же возможно. Такая структура приводит к протяженным кабельным системам, которые связывают конечные узлы или коммутаторы сетей рабочих групп с центральным коммутатором, шина которого и является магистралью сети. Высокая плотность кабелей и их высокая стоимость ограничивают применение стянутой в точку магистрали в таких сетях. Иногда, особенно в сетях кампусов, просто невозможно стянуть все кабели в одно помещение из-за ограничений на длину связей, накладываемых технологией (например, все реализации технологий локальных сетей на витой паре ограничивают протяженность кабелей в 100 м).

Поэтому в локальных сетях, покрывающих большие территории, часто используется другой вариант построения сети - с распределенной магистралью. Пример такой сети приведен на рис 10.

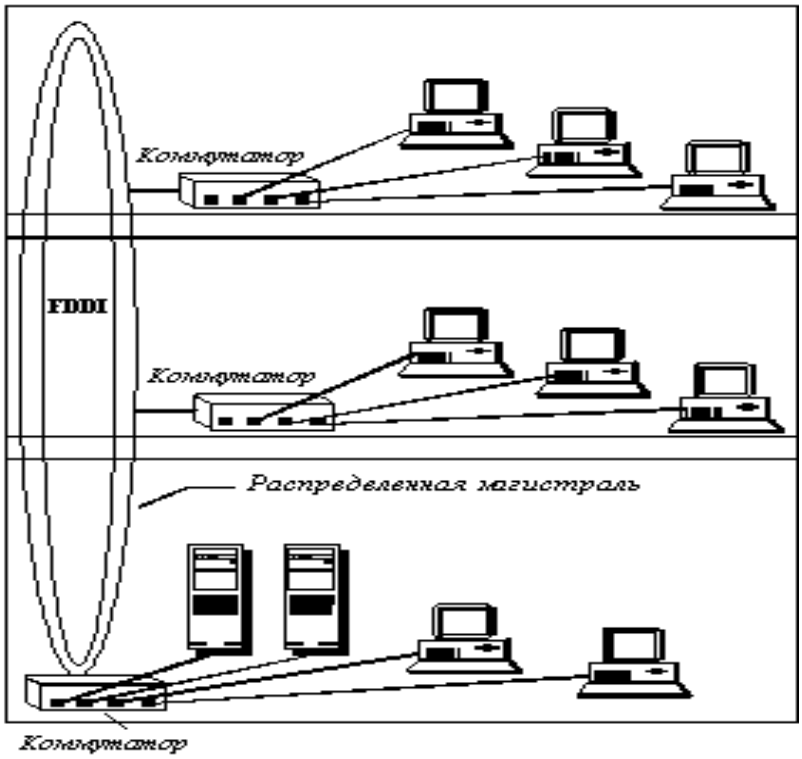


рис. 10 Распределенная магистраль на коммутаторах

2.3 Коммуникационное оборудование сетей

Повторители Ethernet, в контексте сетей 10Base-T, часто называемые концентраторами или хабами, работают в соответствии со стандартом IEEE 802.3. Повторитель просто передает полученные пакеты во все свои порты независимо от адресата.

С точки зрения производительности повторители просто передают пакеты с использованием всей полосы канала. Задержка, вносимая повторителем весьма мала (в соответствии с IEEE 802.3 - менее 3 микросекунд). Сети, содержащие повторители имеют полосу 10 Mbps подобно сегменту на основе коаксиального кабеля и прозрачны для большинства сетевых протоколов, таких как TCP/IP и IPX.

- **Мосты** функционируют в соответствии со стандартом IEEE 802.1d. Подобно коммутаторам Ethernet мосты не зависят от протокола и передают пакеты порту, к которому подключен адресат. Однако, в отличие от большинства коммутаторов Ethernet, мосты не передают фрагменты пакетов при возникновении коллизий и пакеты с ошибками, поскольку все пакеты

буферизуются перед их пересылкой в порт адресата. Буферизация пакетов (store-and-forward) приводит к возникновению задержки по сравнению с коммутацией на лету. Мосты могут обеспечивать производительность, равную пропускной способности среды, однако внутренняя блокировка несколько снижает скорость их работы.

- **Маршрутизаторы** работа маршрутизаторов зависит от сетевых протоколов и определяется связанной с протоколом информацией, передаваемой в пакете. Подобно мостам, маршрутизаторы не передают адресату фрагменты пакетов при возникновении коллизий. Маршрутизаторы сохраняют пакет целиком в своей памяти прежде, чем передать его адресату, следовательно, при использовании маршрутизаторов пакеты передаются с задержкой. Маршрутизаторы могут обеспечивать полосу, равную пропускной способности канала, однако для них характерно наличие внутренней блокировки. В отличие от повторителей, мостов и коммутаторов маршрутизаторы изменяют все передаваемые пакеты.
- **Коммутаторы** Ethernet подобно мостам и маршрутизаторам способны сегментировать сети Ethernet. Как и многопортовые мосты коммутаторы передают пакеты между портами на основе адреса получателя, включенного в каждый пакет. реализация коммутаторов обычно отличается от мостов в части возможности организации одновременных соединений между любыми парами портов устройства - это значительно расширяет суммарную пропускную способность сети. Более того, мосты в соответствии со стандартом IEEE 802.1d должны получить пакет целиком до того, как он будет передан адресату, а коммутаторы могут начать передачу пакета, не приняв его полностью

Хотя все коммутаторы имеют много общего, целесообразно разделить их на два класса, предназначенных для решения разных задач.

Коммутаторы для рабочих групп обеспечивают выделенную полосу при соединении любой пары узлов, подключенных к портам коммутатора.

Если порты имеют одинаковую скорость, получатель пакета должен быть свободен, чтобы не возникло блокировки

Основным преимуществом коммутаторов для рабочих групп является высокая производительность сети на уровне рабочей группы за счет предоставления каждому пользователю выделенной полосы канала (10 Mbps). Кроме того, коммутаторы снижают (в пределе до нуля) количество коллизий - в отличие от магистральных коммутаторов, описанных ниже, коммутаторы рабочих групп, не будут передавать коллизионные фрагменты адресатам. Коммутаторы для рабочих групп позволяют полностью сохранить сетевую инфраструктуру со стороны клиентов, включая программы, сетевые адаптеры, кабели. Стоимость коммутаторов для рабочих групп в расчете на один порт сегодня сравнима с ценами портов управляемых концентраторов.

2.3.1. Аппаратное обеспечение

Корпус Minitower INWIN EMR002 < Black> Micro ATX 350W (24+4пин)

GigaByte GA-H61M-S2PV rev2.1 (RTL) LGA1155 < H61> PCI-E+Dsub+DVI+GbLAN SATA MicroATX 2DDR-III

Процессор CPU Intel Pentium G2020 2.9 ГГц / 2core / SVGA HD Graphics / 0.5+3Мб / 55 Вт / 5 ГТ / с LGA1155

Куллер Arctic Cooling Alpine 11 GT rev.2 Cooler (775 / 1155, 500-2000об / Al)

Оперативная память Crucial < CT25664BA160B> DDR-III DIMM 4Gb < PC3- 12800>

Жесткий диск HDD 500 Gb SATA 6Gb / s Seagate Barracuda 7200.12 < ST500DM002> 3.5" 7200rpm 16Mb

CD-ROM DVD RAM & DVD±R / RW & CDRW Samsung SH-224BB < Black> SATA (OEM)

Картридер Sema < SFD-321F / TS41UB Black> 3.5" Internal USB2.0 CF / MD / xD / MMC / SD / MS(/ Pro / Duo)Card Reader / Writer+1portUSB2.0

Сетевая плата D-Link DGE-528T 100/1000 Mb/s Fast Ethernet PCI Adapter:

Процессор Intel Xeon E5-2650 2.0 ГГц/8core/2+20Мб/95 Вт/8 ГТ/с LGA2011

Жёсткие диски

HDD 1 Tb SATA-II 300 Western Digital RE4 7200rpm 64Mb

HDD Enterprise 3.5” 500Gb 7200 RPM

Память

Kingston ValueRAM DDR-III DIMM 4Gb

Raid-контроллер

Intel RAID Controller RT3WB080 (RTL) PCI-Ex8, SATA-II RAID

ИБП

APC Smart-UPS 1500VA USB & Serial 230V

Шкаф 19"

NT BUSINESS / METAL 24-610 G Шкаф 19" напольный, серый 24U 600x1000. - берем из первой курсовой работы.

Камера видеонаблюдения для улицы PROvision PV-IR600D1

Профессиональная уличная цветная камера видеонаблюдения PROvision PV-IR600D1 оснащена фиксированным объективом, мощной ИК-подсветкой, высококачественной матрицей.

Камера видеонаблюдения для помещения Alert APD-420H1 (Fix-3,6) 420 ТВЛ; CMOS PixelPlus PC1030; 3,6мм; 0,5 люкс; BNC; DC 12V 0,3A; -10...+50 °C.

Медиаконвертер (транспондер) 8-канальный STM, ATM, Gigabit Ethernet 1U без SFP трансиверов, напряжение питания 36..72В и 220В, управление по SNMP и Web.

Плата видеозахвата Интеллект D8 (2FS15) / D8 (FX4)

Интеллект D8 (2FS15) / D8 (FX4) - система видеонаблюдения 8 каналов 4 к/с на канал

Wi-Fi роутер.

Сетевой WiFi адаптер(сетевая карта, сетевой адаптер, контроллер, net card, network card, network adapter) – это оборудование, которое используются для подключения к беспроводным сетям устройств, не имеющих встроенного WiFi-модуля — стационарных компьютеров, телевизоров, игровых приставок и др.

Сетевая розетка. При прокладке сети в помещении на витой паре используются специальные розетки, к которым идет кабель от сетевого устройства.

Телефонная розетка.

При наличии телефонной связи в помещении используются телефонные розетки для подключения проводов абонентской линии.

В целях экономии будут использованы комбинированные розетки компании «EL-BI».

Силовая розетка.

В офисах комбинированная розетка будет состоять из силовой и сетевой.

Комбинированные рамки.

Используются для размещения в кабель-канале различных розеток (силовая, информационная, телефонная и т.п.).

Коннектор RJ-11.

Телефонный унифицированный разъём. RJ-11 использует стандартный шестиконтактный разъем, применяемые в телефонии, однако реально используется только два центральных контакта.

Коннектор RJ-45.

Универсальные коннекторы RJ-45 предназначены для окольцовки кабеля типа UTP/FTP.

Телефонный кабель.

3. НАСТРОЙКИ СЕТИ НА СОС UBUNTU SERVER

3.1 Настройка DNS-сервера

Шаг первый: Установка DNS

На этом шаге в терминале прописываем команду

sudo apt-get install bind9

DNS-пакеты устанавливаются.

Шаг второй: Создание секретного ключа

На этом шаге создаём секретный ключ, который понадобиться для обновления DNS-записей в зоне нашей локальной сети. Прописываем команду :

dnssec-keygen -a HMAC-MD5 -b 128 -r /dev/urandom -n USER DHCP_UPDATER

Проверим, что у нас получилось командой

cat Kdhcp_updater.*.private|grep Key

Получаем : Key: cYqlx8g/jLcIxXFDpqrxZw==

Шаг третий: Настройка сетевого соединения со статическим IP

На этом шаге вносим изменения в файл **/etc/network/interfaces**

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet static

address 192.168.0.2

#hwaddress ether 00:01:2e:2c:d6:70

netmask 255.255.255.0

network 192.168.0.0

broadcast 192.168.0.255

gateway 192.168.0.1

dns-nameservers 192.168.0.2

The secondary network interface

#auto wlan1

#iface wlan1 inet static

address 192.168.0.12

#hwaddress ether 00:25:d3:f0:c2:92

netmask 255.255.255.0

gateway 192.168.0.1

Адрес DNS сервера можно задать в файле **/etc/network/interfaces** , но вообще управление адресами DNS серверов в Ubuntu осуществляется через файл **/etc/resolv.conf**. Важно не забыть его поправить. Он должен иметь вид:

domain team.local

search team.local

nameserver 127.0.0.1

Перезапускаем службу **networking**

/etc/init.d/networking restart

Шаг четвертый : Настройка bind9

На этом шаге нам нужно отредактировать 2 файла: **named.conf.options** и **named.conf.local**

Правим **named.conf.options** :

forwarders {

8.8.8.8;

8.8.4.4;

204.194.232.200;

204.194.234.200;

};

listen-on {

127.0.0.1;

192.168.0.2;

};

Теперь редактируем **named.conf.local** (вводим сгенерированный ранее ключ) :

```
key DHCP_UPDATER {
algorithm HMAC-MD5.SIG-ALG.REG.INT;
secret cYqlx8g/jLcIxXFDpqrxZw==;
};
zone "team.local" IN {
type master;
file "/var/lib/bind/forward.bind";
allow-update { key DHCP_UPDATER; };
};
zone "0.168.192.in-addr.arpa" IN {
type master;
file "/var/lib/bind/reverse.bind";
allow-update { key DHCP_UPDATER; };
};
```

Шаг пятый : Создание прямой и обратной зоны для сети.

В папке **/var/lib/bind** создаём файл для прямой зоны, назовём его **forward.bind**. Файл используется DNS-сервером для преобразования имени компьютеров локальной сети в ip-адрес.

```
$TTL 86400 ; 1 day
team.local. IN SOA ns1.team.local. admin.team.local. (
20110103 ; Serial
10800 ; Refresh
3600 ; Retry
604800 ; Expire
86400 ; Minimum TTL
)
IN NS ns1.team.local.
IN A 192.168.0.2
```

localhost IN A 127.0.0.1

ns1 IN A 192.168.0.2

gw IN A 192.168.0.1

Далее создаём файл для обратной зоны, **reverse.bind**. Файл используется DNS-сервером для преобразования ip-адреса компьютеров локальной сети в доменное имя. $TTL 86400 ; 1 day

0.168.192.in-addr.arpa. IN SOA ns1.team.local. admin.team.local. (

20110104 ; Serial

10800 ; Refresh

3600 ; Retry

604800 ; Expire

3600) ; Minimum

IN NS ns1.team.local.

1 IN PTR gw.team.local.

2 IN PTR team.local.

2 IN PTR ns1.team.local.

Шаг шестой : перезапускаем bind9 командой

/etc/init.d/bind9 restart

Аудитория	Name	IP-address	DNS	Gateaway
101	OHRANA101	196.34.19.161	192.168.0.254	192.168.0.1
102	SMenedger102-1	196.34.19.162	192.168.0.254	192.168.0.1
102	SMenedger102-2	196.34.19.163	192.168.0.254	192.168.0.1
102	SMenedger102-3	196.34.19.164	192.168.0.254	192.168.0.1
102	SMenedger102-4	196.34.19.165	192.168.0.254	192.168.0.1
102	SMenedger102-5	196.34.19.166	192.168.0.254	192.168.0.1
103	Kassa103-1	196.34.19.167	192.168.0.254	192.168.0.1
103	Buhgalter103-2	196.34.19.168	192.168.0.254	192.168.0.1
104	SysAdmin104	196.34.19.169	192.168.0.254	192.168.0.1
105	GBuhgalter105	196.34.19.170	192.168.0.254	192.168.0.1
106	Secretar106	196.34.19.171	192.168.0.254	192.168.0.1
106	KMenedger106	196.34.19.172	192.168.0.254	192.168.0.1
107	Director107	196.34.19.173	192.168.0.254	192.168.0.1
108	ZAL108	196.34.19.174	192.168.0.254	192.168.0.1

3.2 Настройка DHCP сервера

Шаг первый: Установка DHCP сервера

На этом шаге в терминале прописываем команду

sudo apt-get install dhcp3-server и начнётся установка сервера.

Шаг второй: Настройка сервера

На этом шаге прописываем команду :

sudo nano /etc/dhcp3/dhcpd.conf **-открываются настройки конфигурации dhcp сервера. Имя сети, можно оставить как есть, но лучше закомментировать.**

#option domain-name "example.org";

#option domain-name-servers ns1.example.org, ns2.example.org;

Если данный DHPC сервер будет единственным в сети, то директиву лучше раскоментировать.

authoritative;

Далее находим диапазон настроек адресов:

Снимем комментарии со строчек, которые нам необходимы:

A slightly different configuration for an internal subnet.

subnet 192.168.0.0 netmask 255.255.255.0 { # подсеть и маска

range 192.168.0.5 192.168.0.254; # **- указываем диапазон IP адресов, которые будут выдаваться клиентам**

option domain-name-servers 192.168.0.2; # IP DNS-сервера

option domain-name "internal.example.org"; # **- можно задать название своей сети**

option routers 192.168.0.1;# **- адрес шлюза или маршрутизатора через который мы выходим в Интернет.**

option broadcast-address 192.168.0.255;# **- широковещательный адрес который находится последним в диапазоне IP данной подсети**

default-lease-time 600;# **время аренды IP адреса в сек.**

max-lease-time 7200; # **максимальное время аренды IP адреса**

3.3. Установка и настройка FTP - сервера и привязка к локальным пользователям

Vsftpd есть в репозиториях Ubuntu поэтому поставить его проще простого, в консоли набираем:

sudo apt-get install vsftpd

Теперь займемся конфигом :

Особенности конфига: запрещен анонимный доступ, назначен стандартный порт для прослушивания, разрешены локальные пользователи, umask назначен 002 (это значит что все залитые по фтп файлы будут иметь права 664), разрешено изменение прав доступа к файлам по фтп включая рекурсию, пользователям запрещен выход из домашней папки.

Настройка **ftp сервера** на этом заканчивается.

Теперь займемся пользователями :

Настройка пользователей :

Переходим в **/etc/shells**:

sudo gedit /etc/shells

В конец добавляем строку:

/bin/false

Сохраняем, закрываем .

Теперь надо создать **2 группы**, одна группа (web-users) будет для пользователей, другая (web-developers) для разработчиков

sudo addgroup web-users && sudo addgroup web-developers

Далее необходимо добавить сервер **apache** в каждую из созданных групп (по умолчанию **apache** работает под пользователем www-user):

sudo useradd www-user web-users && sudo useradd www-user web-developers

Теперь необходимо настроить самих пользователей.

Создаем папки для будущих пользователей :

Для удобства в папке /home создаем папки для каждой из групп:

sudo mkdir /home/web-developers && sudo mkdir /home/web-users

Теперь предположим что логины наших пользователей – user1, dev1, dev2 создадим папки для пользователей:

sudo mkdir /home/web-users/user1

sudo mkdir /home/web-developers/dev1

sudo mkdir /home/web-developers/dev2

Теперь создадим пользователей а заодно сразу раскидаем их по нужным группам:

sudo useradd user1 -g web-users -p 217ulumap -d /home/web-users/user1 -s /bin/false

sudo useradd dev1 -g web-developers -p 217ulumap -d /home/web-developers/dev1 -s /bin/false sudo useradd dev2 -g web-developers -p 217ulumap -d /home/web-developers/dev2 -s /bin/false

Такая конструкция создаст пользователей которые не смогут авторизоваться в системе, однако смогут использовать ftp сервер как положено.

Теперь **назначим пользователей владельцами папок** созданных ранее:

sudo chown user1:web-users /home/web-users/user1 sudo chown dev1:web-developers /home/web-developers/dev1 sudo chown dev2:web-developers /home/web-developers/dev2

Предположим, что **есть 2 сайта** которые лежат в /var/www – **site1.com и site2.com**

Первый принадлежит пользователю, а второй находится на разработке у программеров. Чтобы раздать эти сайты необходимо промонтировать их в домашние директории пользователей. Для этого необходимо сначала создать соответствующие папки в домашних папках пользователей, а потом уже примонтировать туда файлы наших сайтов.

sudo mkdir /home/web-users/user1/site1.com sudo chown user1:web-users /home/web-users/user1/site1.com sudo mkdir /home/web-

developers/dev1/site2.com sudo chown dev1:web-developers /home/web-developers/dev1/site2.com sudo mkdir /home/web-developers/dev2/site2.com sudo chown dev2:web-developers /home/web-developers/dev2/site2.com

Теперь добавляем точку монтирования для каждого из пользователей, для этого правим **fstab**:

sudo gedit /etc/fstab

Добавляем нужные пути:

/var/www/site1.com /home/web-users/user1/site1.com none bind 0 0

/var/www/site2.com /home/web-developers/dev1/site2.com none bind 0 0

/var/www/site2.com /home/web-developers/dev2/site2.com none bind 0 0

Перезагружаемся и радуемся результату.

3.4 Установка Apache2, MySQL, PHP

Установка mysql:

sudo apt-get install mysql-server mysql-client

ps –ef | grep mysql

Установка Apache2 :

sudo apt-get install apache2

ps -ef | grep apache2

Теперь ставим PHP :

sudo apt-get install php5 libapache2-mod-php5

Перезапускаем apache2 :

/etc/init.d/apache2 restart

После перезапуска нам необходимо создать пустой php файл, и вписать в него несколько строк, для начала нам необходимо задать дериктории /var/www/ права на запись и редактирование файлов, что бы в дальнейшем не возникали различные казусы

cd /var/www/

sudo chmod /var/www/ -R 777 ./

Теперь, не выходя из этой директории можно создать наш php файл

touch index.php

nano index.php

И вписываем туда код, как показано на скриншоте ниже:

Вводим в браузере **http://localhost/index.php** и наблюдаем :

sudo apt-get install php5-mysql php5-curl php5-gd php5-idn php-pear php5-imagick php5-imap php5-mcrypt php5-memcache php5-ming php5-ps php5-pspell php5-recode php5-snmp php5-sqlite php5-tidy php5-xmlrpc php5-xsl

Перезагружаем apache2 :

/etc/init.d/apache2 restart

Перезагружаем нашу страницу **http://localhost/index.php** и у нас должны появится пункты mysql и mysqli

На этом установка MySQL, APACHE2 и PHP завершена.

3.5 Настройка прокси-сервера SQUID

Шаг первый: Установка SQUID

sudo apt update

После обновления списка пакетов можно переходить к установке прокси-сервера просто выполните команду:

На этом шаге в терминале прописываем команду sudo apt-get install squid и squid устанавливается.

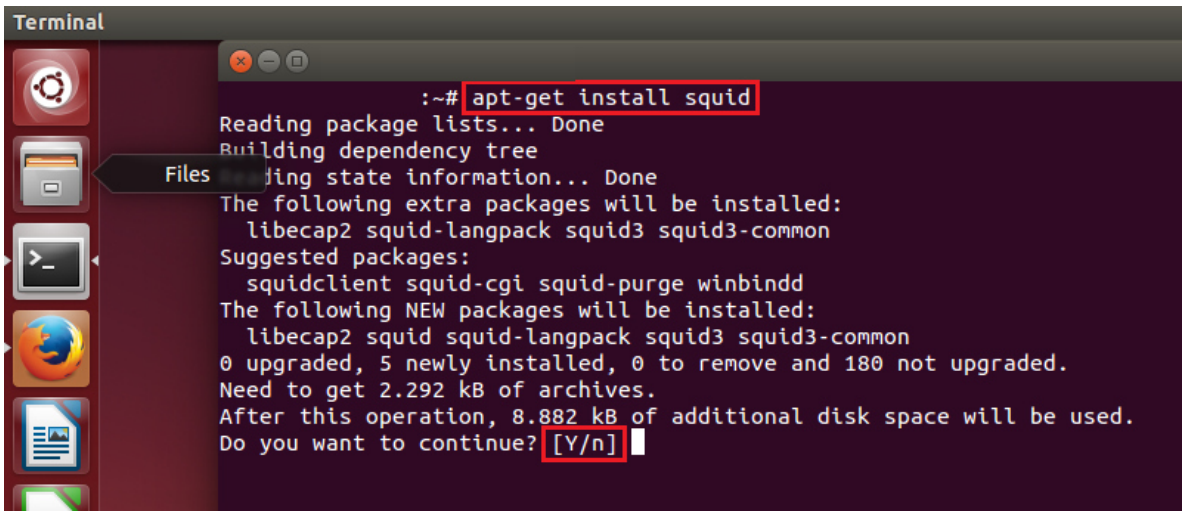


Рис 11 - Установка SQUID

Шаг второй: Настройка SQUID

Конфигурационный файл сервера находится в директории /etc/squid. В зависимости от версии Squid название папки и самого файла может отличаться, например, /etc/squid3/squid.conf или /etc/squid/squid.conf. Все настройки находятся в этом файле. Давайте его рассмотрим.

На этом шаге прописываем команду sudo nano /etc/squid/squid.conf открывается файл конфигурации squid. По умолчанию SQUID использует для работы порт 3128, но нам необходимо сделать так чтобы не было необходимо перенастраивать каждого клиента, для этого необходимо использовать

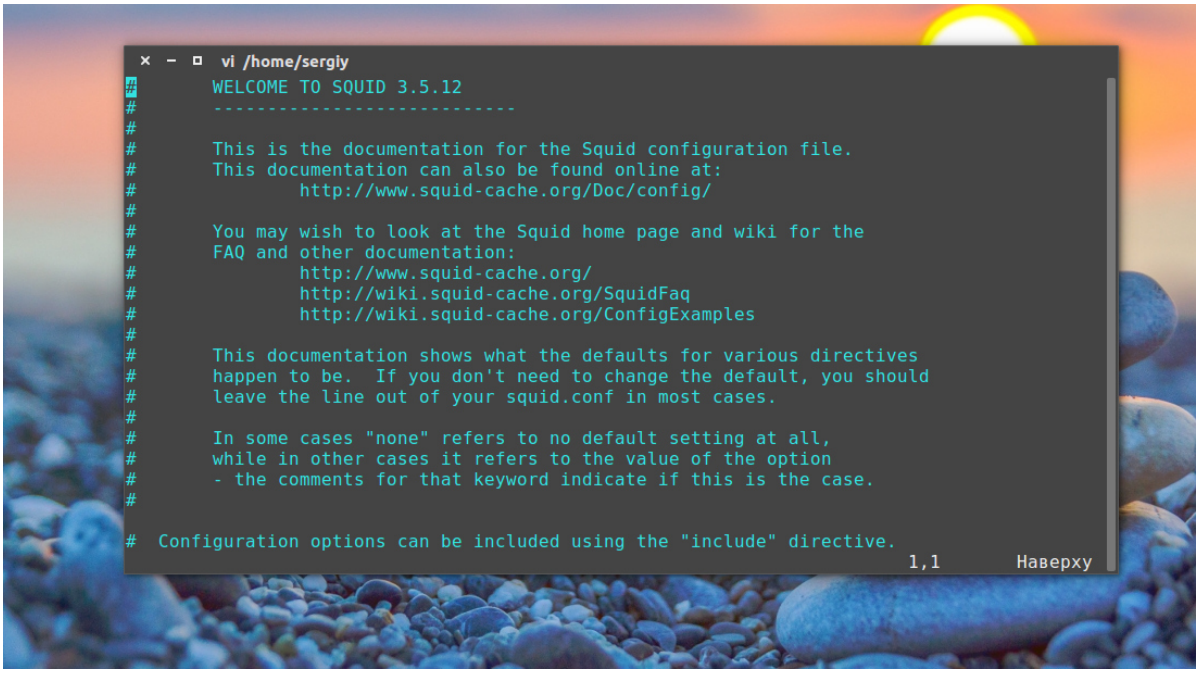


Рис 12 - Файл конфигурации

Файл содержит несколько опций настроек, а также очень много документации по их использованию. Мы не будем трогать многие из них, но основные рассмотрим. Сначала нам нужно настроить правила доступа клиентов к нашему прокси-серверу. Squid проектировался как программа для организаций и даже если вы используете его дома, настройка squid 3 тоже должна быть выполнена.

Для это используется acl список. это обычный список объектов, сейчас он вообще ничего не значит. Это могут быть ip адреса, порты и т д. Потом мы укажем программе что нужно делать с этим списком, разрешать или запрещать доступ. Синтаксис создания acl списка такой:

Таких строк может быть несколько с одним именем и типом, из них получается список. Имя списка может быть произвольным, мы его еще будем использовать. Тип списка это намного интереснее. Может быть одним из:

- **src** - ip адрес откуда исходит соединение, адрес клиента;
- **dst** - ip адрес назначения соединения, адрес сервера, к которому хочет получить доступ клиент;
- **dstdomain** - домен назначения соединения;
- **srcdomain** - домен клиента;
- **arp** - MAC адрес сетевой карты клиента;
- **time** - время, когда выполняется соединение;
- **port** - порт, к которому пытается получить доступ клиент;
- **proto** - протокол, по которому устанавливается соединение;
- **method** - метод передачи данных, например, GET - передача данных HTTP, POST - передача данных форм в HTTP, CONNECT - запрос соединения с сервером;

- **http_status** - ответ сервера;
- **browser** - браузер клиента;
- **url_regex** - url адрес, к которому пытаются получить до

Добавим список, для доступа к серверу из локальной сети:

acl localnet src 192.168.0.0/16

Создадим список Safe_ports, чтобы разрешить трафик на порты основных сетевых служб, а также незарегистрированные порты выше 1024:

```
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
```

Создадим еще два списка - SSL_ports и connect, чтобы разрешить использовать метод connect только для ssl соединений. Это запретит клиенту использовать другие прокси-серверы поверх нашего:

```
acl SSL_ports port 443
```

Шаг третий : Повышение безопасности сервера

```
linus@linux:~$ sudo apt install --fix-broken
Reading package lists... Done
Building dependency tree
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
1 not fully installed or removed.
After this operation, 0 B of additional disk space will be used.
Setting up rabbitmq-server (3.6.10-1) ...
Job for rabbitmq-server.service failed because the control process exited with error code.
See "systemctl status rabbitmq-server.service" and "journalctl -xe" for details.
invoke-rc.d: initscript rabbitmq-server, action "start" failed.
● rabbitmq-server.service - RabbitMQ Messaging Server
   Loaded: loaded (/lib/systemd/system/rabbitmq-server.service; enabled; vendor preset: enabled)
   Active: failed (Result: exit-code) since Sun 2018-11-11 13:47:26 MSK; 9ms ago
  Process: 5486 ExecStartPost=/usr/lib/rabbitmq/bin/rabbitmq-server-wait (code=exited, status=70)
  Process: 5485 ExecStart=/usr/sbin/rabbitmq-server (code=exited, status=0/SUCCESS)
 Main PID: 5485 (code=exited, status=0/SUCCESS)

ноя 11 13:47:21 linux systemd[1]: Starting RabbitMQ Messaging Server...
ноя 11 13:47:24 linux rabbitmq[5486]: Waiting for rabbit@linux
ноя 11 13:47:24 linux rabbitmq[5486]: pid is 5502
ноя 11 13:47:26 linux rabbitmq[5486]: Error: process_not_running
ноя 11 13:47:26 linux systemd[1]: rabbitmq-server.service: Control process exited, code=exited status=70
ноя 11 13:47:26 linux systemd[1]: rabbitmq-server.service: Failed with result 'exit-code'.
ноя 11 13:47:26 linux systemd[1]: Failed to start RabbitMQ Messaging Server.
dpkg: error processing package rabbitmq-server (--configure):
 installed rabbitmq-server package post-installation script subprocess returned error exit status 1
Errors were encountered while processing:
 rabbitmq-server
E: Sub-process /usr/bin/dpkg returned an error code (1)
linus@linux:~$
```

Рис 12 - Повышение безопасности сервера

На этом шаге находим следующий блок:

```
#               acl fileupload req_mime_type -i ^multipart/form-data$
#               acl javascript rep_mime_type -i ^application/x-javascript$
#
#Default:
# acl all src all
#
#       I
# Recommended minimum configuration:
#
acl lan src 192.168.1.0/24
acl sblock url_regex "/etc/squid3/block"
acl manager proto cache_object
acl localhost src 127.0.0.1/32 ::1
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32 ::1

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
#acl localnet src 10.0.0.0/8    # RFC1918 possible internal network
```

Рис 13. Блок squid

#acl localnet src 10.0.0.0/24 # RFC1918 possible internal network

#acl localnet src 172.16.0.0/12 # RFC1918 possible internal network

#acl localnet src 192.168.0.0/16 # RFC1918 possible internal network

Для повышения безопасности сервер будет обслуживать запросы только из локальной сети, IP адреса в моей локальной сети из диапазона

192.168.1.0/24, Где: 192.168.1.0-подсеть, /24-количество бит в маске-идентификаторе сети (255.255.255.0)

#acl localnet src 10.0.0.0/24 # RFC1918 possible internal network

#acl localnet src 172.16.0.0/12 # RFC1918 possible internal network

acl localnet src 192.168.1.0/24 # RFC1918 possible internal network

Разрешаем доступ из localnet: http_access allow localnet

Находим и раскоментируем, правило кеширования

cache_dir ufs /var/spool/squid 4096 32 256 всё остальное можно оставить как есть.

8. ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕЧПЕЧЕНИЯ

Таблица 13 - Программное обеспечение

Программное обеспечение	Цена
Office 2010 Win32 Russian AE CD	3 417
MS Windows 7Russian Second Edition	2 379
Kaspersky antivirus CRYSTAL 2.0	2 200/2 комп
AutoCAD LT Commercial Subscription	5 678
FrontPage 2010 English Intl AE CD	2 257
По для видеокамер "Интеллект"	15 200
СОС Ubuntu Server 10.10	
Общая сумма	31 131

3.3. Конфигурация сетевого оборудования

1. Настройка коммутатора:

Создание VLAN’а и задание имени :

SW1> en

SW1# conf t

SW1(config)# vlan 2

SW1(config-vlan)# name DIR (Директор)

SW1(config-vlan)# exit

SW1(config)# vlan 3

SW1(config-vlan)# name BUCH (Бухгалтер)

SW1(config-vlan)# exit

SW1(config)# vlan 4

SW1(config-vlan)# name PERSONAL (Персонал)

SW1(config-vlan)# exit

SW1(config)# vlan 5

SW1(config-vlan)# name SEC (Охранник)

SW1(config-vlan)# exit

SW1(config)# vlan 11

SW1(config-vlan)# name SYS (Системный администратор)

SW1(config-vlan)# exit

Теперь присваеваем каждому VLAN’у свою группу ПК :

SW1(config)#int range fa 0/10 – **определяем группу интерфейсов;**

SW1 (config-if-range)#switchport mode access – **задаем режим интерфейсам;**

SW1 (config-if-range)#switchport access vlan 3 – **определяем интерфейсы соответствующему vlan;**

SW1 (config-if-range)#exit

SW1 (config)#int range fa 0/13

SW1 (config-if-range)#switchport mode access

SW1 (config-if-range)#switchport access vlan 2

SW1 (config-if-range)#exit

SW1 (config-if)#switchport mode trunk – **определяем интерфейс как trunk;**

SW1 (config-if)#exit

SW1 (config)#vtp mode server – **определяем коммутатору роль Server в VTP;**

Device mode already VTP SERVER.

SW1 (config)#vtp domain sanek – **задаем имя VTP домену (должно быть одинаково на всех коммутаторах);**

Changing VTP domain name from NULL to sanek

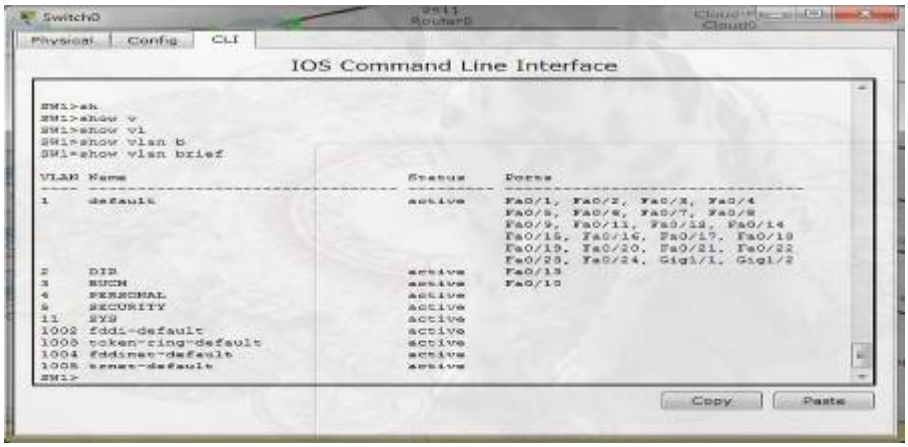
SW1 (config)#vtp password 217ulumap – **задаем пароль для VTP (должен быть одинаковым на всех коммутаторах);**

Setting device VLAN database password to 217ulumap

SW1 (config)#vtp version 2 – **определяем версию VTP (должна быть одинаковая на всех коммутаторах);**

Switch_1(config)#exit

SW1#wr



Переходим к настройке SW2:

R2>en

R2#conf t

R2(config)#host

R2(config)#hostname SW2

SW2 (config)#vtp mode transparent – **ставим соответствующий режим VTP;**

Setting device to VTP TRANSPARENT mode.

SW2 (config)#vtp version 2

SW2 (config)#vtp domain sanek

Changing VTP domain name from NULL to sanek

SW2 (config)# vtp password 217ulumap

Setting device VLAN database password to 217ulumap

SW2(config)#int range fa 0/2 - 8

SW2 (config-if-range)#switchport mode access

SW2 (config-if-range)#switchport access vlan 4

SW2 (config-if-range)#exit

SW2 (config)#int range fa 0/11 - 12

SW2 (config-if-range)#switchport mode access

SW2 (config-if-range)#switchport access vlan 4

SW2 (config-if-range)#exit

SW2 (config)#int fa 0/14

SW2 (config-if-range)#switchport mode access

SW2 (config-if-range)#switchport access vlan 4

SW2 (config-if-range)#exit

SW2 (config)#int fa 1/0

SW2 (config-if)#switchport mode trunk

SW2 (config-if)#switchport trunk encapsulation dot1q

SW2 (config-if)#exit

SW2 (config)#int fa 1/1

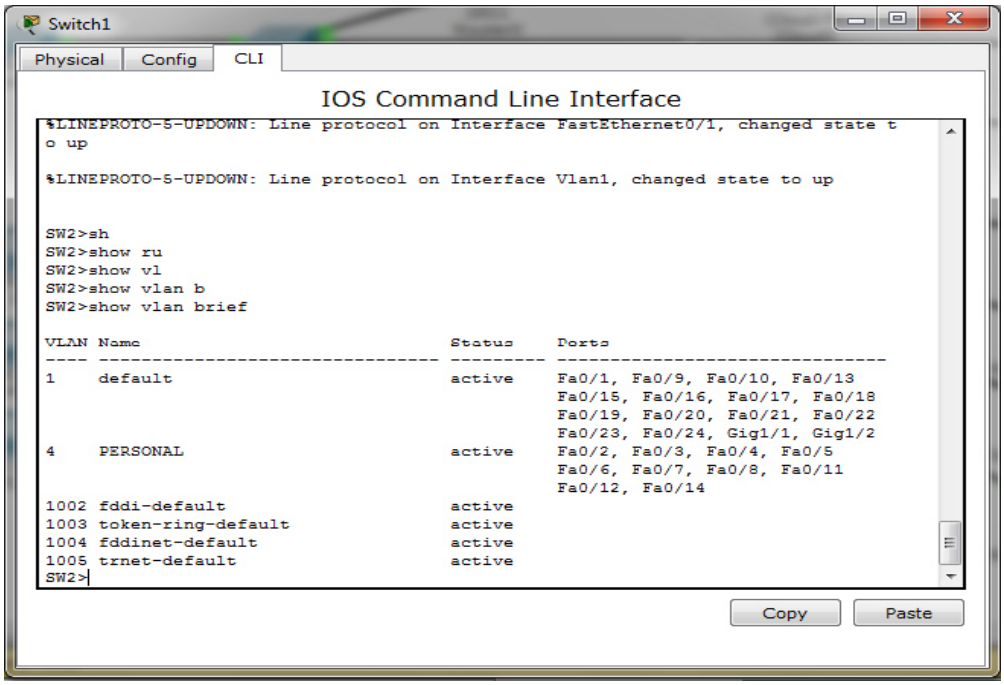
SW2 (config-if)#switchport mode trunk

SW2 (config-if)#switchport trunk encapsulation dot1q

SW2 (config-if)#exit

SW2 (config)#exit

SW2#wr



Теперь, перейдем к настройкам SW3:

R3>en

R3#conf t

R3(config)#host

R3(config)#hostname SW3

SW3 (config)#int vlan 1

SW3 (config-if)#ip address 192.168.1.3 255.255.255.0

SW3 (config-if)#no shutdown

SW3 (config-if)#exit

SW3 (config)#vtp version 2

SW3 (config)#vtp mode client

Setting device to VTP CLIENT mode.

SW3 (config)#vtp domain sanek

Changing VTP domain name from NULL to sanek

SW3 (config)#vtp password 217ulumap

Setting device VLAN database password to 217ulumap

SW3 (config)# int fa 1/1

SW3 (config-if)# switchport mode trunk

SW3 (config-if)# switchport trunk encapsulation dot1q

SW3 (config-if)# exit

SW3 (config)# exit

SW3#wr

Таблица 15 – Распределение пользователей на VLAN’ы

ПК	VLAN	IP-address	Порт	Пользователь
PC0	5	196.34.19.161	FastEthernet 0/1	Охранник
PC1	4	196.34.19.162	FastEthernet 0/2	Менеджер 1
PC2	4	196.34.19.163	FastEthernet 0/3	Менеджер 2
PC3	4	196.34.19.164	FastEthernet 0/4	Менеджер 3
PC4	4	196.34.19.165	FastEthernet 0/5	Менеджер 4
PC5	4	196.34.19.166	FastEthernet 0/6	Менеджер 5
PC6	4	196.34.19.167	FastEthernet 0/7	Бухгалтер
PC7	4	196.34.19.168	FastEthernet 0/8	Кассир
PC8	11	196.34.19.169	FastEthernet 0/9	Сис. Администратор
PC9	3	196.34.19.170	FastEthernet 0/10	Гл. Бухгалтер
PC10	4	196.34.19.171	FastEthernet 0/11	Секретарь
PC11	4	196.34.19.172	FastEthernet 0/12	Менеджер по кадрам
PC12	2	196.34.19.173	FastEthernet 0/13	Директор
PC13	4	196.34.19.174	FastEthernet 0/14	Конференц-зал

2. Настройка Роутера :

Создание имя пользователя и пароля:

R1>enable

R1#configure terminal

R1(config)#

Теперь зададим имя нашему устройству. Делается это командой:

R1(config)# username sanek privilege 15 secret 217ulumap

Дальше настроим имя и пароль администратора и зададим пароль на вход в режим глобальной конфигурации:

sanek (config)#username sanek password 217ulumap

sanek (config)#enable secret 217ulumap

По умолчанию, шифруется только пароль для входа в режим глобальной конфигурации, остальные пароли хранятся в открытом виде. Для их шифрования используется следующая команда:

sanek (config)#service password-encryption

Проходим авторизацию :

aaa new-model

aaa authentication login default local

aaa authorization exec default local

aaa authorization network default local

Теперь настроим наши линии vty и console. Для этого зайдем в режим конфигурирования линий vty и настроим аутентифицировать нас, используя локальную базу (username и password, которые мы задавали чуть выше), использовать для подключения telnet и ssh, время простоя сессии 10 минут и параметр «возвращения каретки» при вводе команд и выдаче системных сообщений:

sanek (config)# line vty 0 14

sanek (config-line)# login local

sanek (config-line)# transport input telnet ssh

sanek (config-line)# exec-timeout 10

sanek (config-line)# logging synchronous

sanek (config-line)# exit

Теперь заходим в режим конфигурирования линий console и делаем те же настройки (кроме параметров telnet и ssh):

sanek (config)# line console 0

sanek (config-line)# login local

sanek (config-line)# logging synchronous

sanek (config-line)# exec-timeout 10 0

sanek (config-line)# exit

Зададим баннер, который будет отображаться при входе на роутер:

sanek (config)#banner login c <HELLOcSANEK)>

c – это баннер при входе на роутер («c» - это разделитель, его наличие обязательно).

Для того чтобы роутер не пытался «разрешить» неопознанные команды с локальным именем и не тормозил нам работу, введем следующее:

sanek (config)#no ip domain-lookup

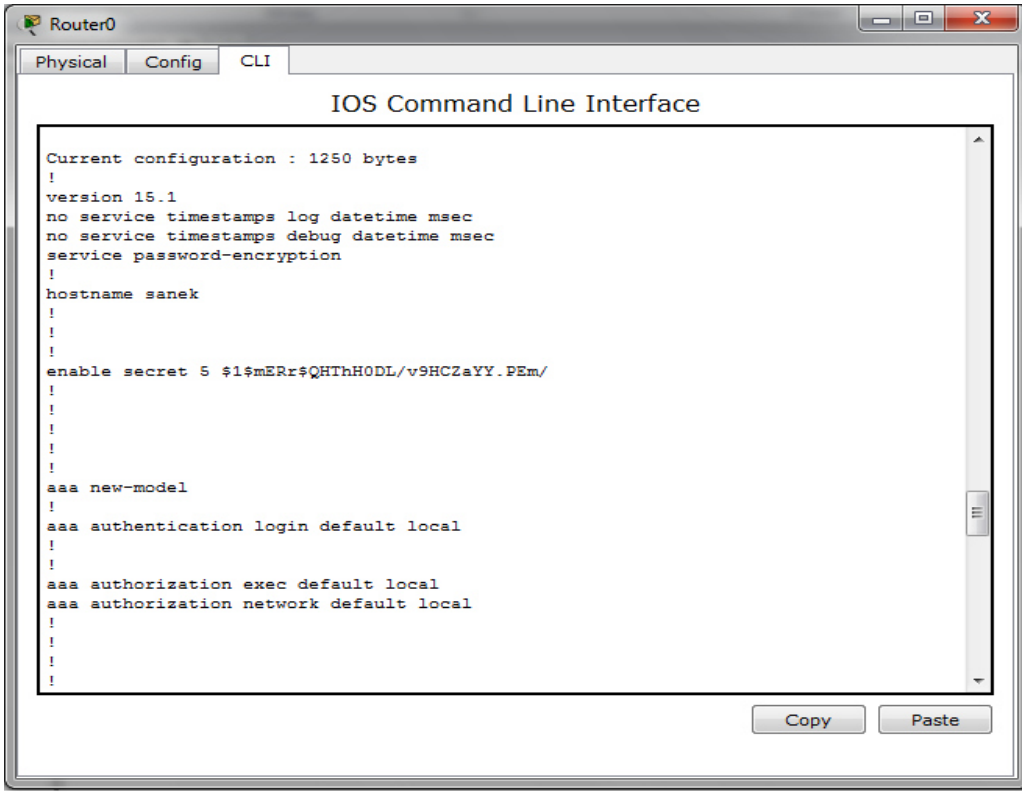
Сохраним конфигурацию. Для этого можно выйти в привилегированный режим, набрав exit, а можно использовать сочетание «do» перед командой:

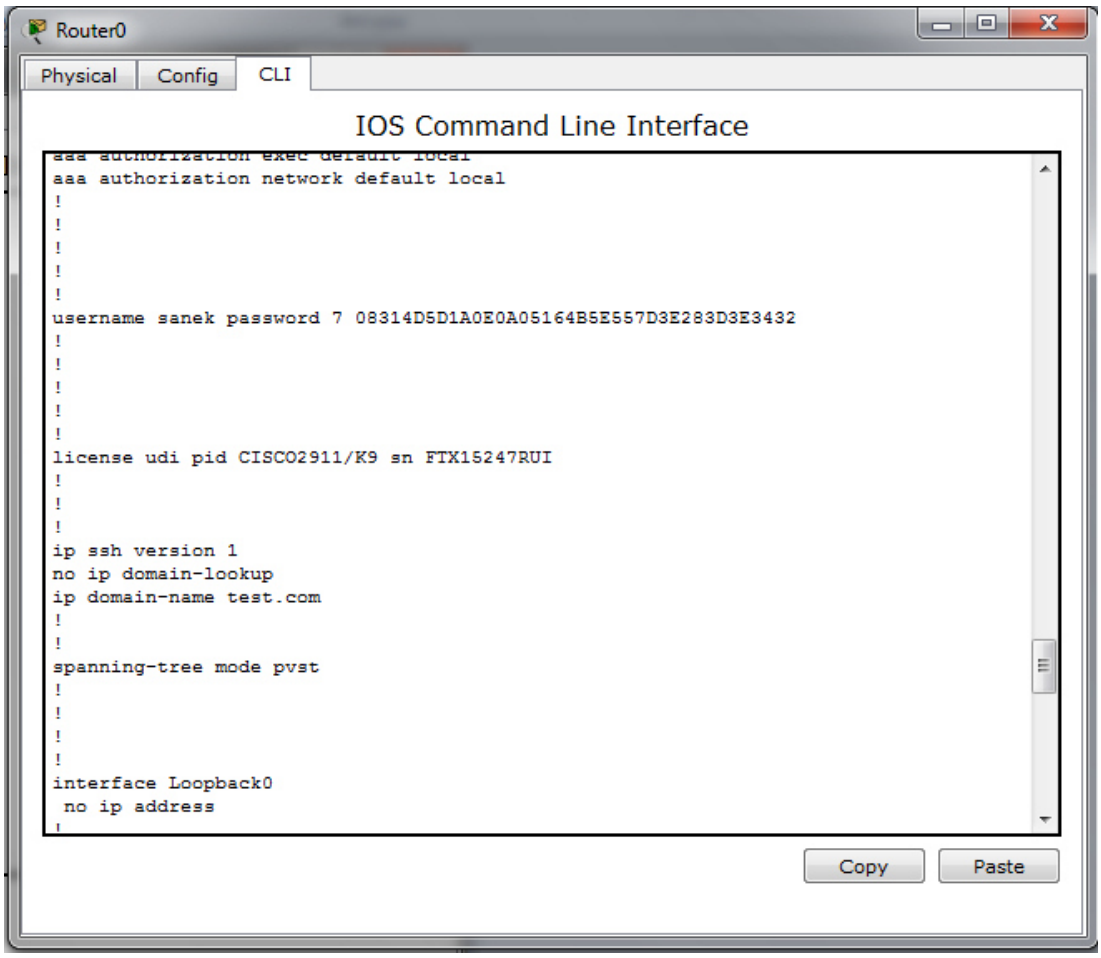
sanek(config)#do wr

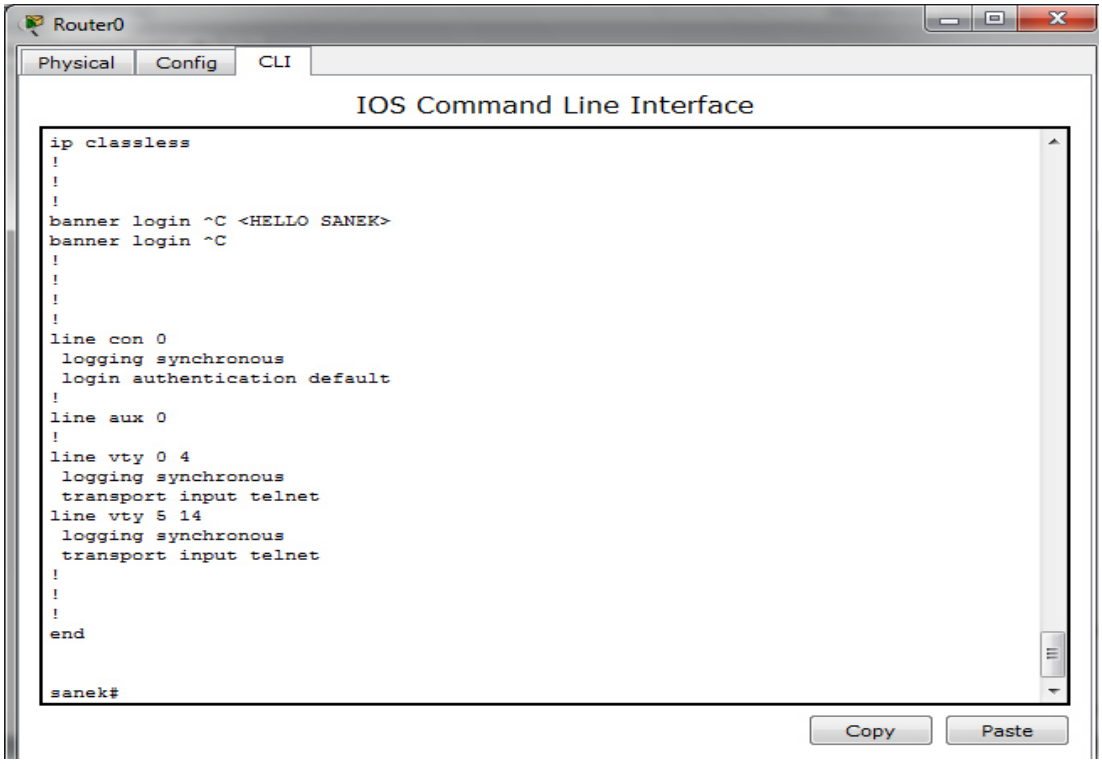
Building configuration...

[OK]

sanek(config)# exit sanek# show running –config




Router0
Physical
Config
CLI
IOS Command Line Interface
aaa authorization exec default local
aaa authorization network default local
!
!
!
!
!
username sanek password 7 08314D5D1A0E0A05164B5E557D3E283D3E3432
!
!
!
!
!
license udi pid CISCO2911/K9 sn FTX15247RUI
!
!
!
ip ssh version 1
no ip domain-lookup
ip domain-name test.com
!
!
spanning-tree mode pvst
!
!
!
!
interface Loopback0
no ip address
Copy
Paste


Router0
Physical
Config
CLI
IOS Command Line Interface
ip classless
!
!
!
banner login ^C <HELLO SANEK>
banner login ^C
!
!
!
!
line con 0
logging synchronous
login authentication default
!
line aux 0
!
line vty 0 4
logging synchronous
transport input telnet
line vty 5 14
logging synchronous
transport input telnet
!
!
!
end
sanek#
Copy
Paste

Теперь, давайте сделаем доступ по telnet и ssh. Для начала, настроим ip – адрес, на который мы будем подключаться.

Заходим в настройки любого интерфейса и, собственно говоря, настраиваем IP-адрес :).

Router_1#conf t

Router_1(config)#int fa 0/0

Router_1(config-if)#ip address 192.168.0.1 255.255.255.0

Router_1(config-if)#no shutdown

Router_1(config-if)#exit

Router_1(config)#

Теперь, доработаем конфигурацию ssh. Надо сгенерировать пару ключей. Для их генерации используется имя домена. Необходимо выполнить следующие действия:

Router_1(config)#ip domain-name test.com

Router_1(config)#crypto key generate rsa

1024

Для проверки подключаемся по ssh через PUTTY

3. Настройка VoIP:

Как обычно, настроим сетевую доступность. Начнем с коммутаторов SW1:

R1>en

R1#conf t

R1(config)# hostname SW1

SW1 (config)# exit

SW1# vlan database – **заходим в режим создания нужных vlan-ов**;

SW1 (vlan)# vlan 2 name DIR

SW1 (vlan)# vlan 3 name BUCH

SW1 (vlan)# exit

SW1# conf t

SW1 (config)# int fa 1/0

SW1 (config-if)# switchport mode access – **определяем нужные порты в нужные vlan**;

SW1 (config-if)# switchport access vlan 2

SW1 (config-if)#exit

SW1 (config)# int fa 1/1

SW1 (config-if)# switchport mode access

SW1 (config-if)# switchport access vlan 3

SW1 (config-if)# exit

SW1 (config)# int fa 1/15

SW1 (config-if)# switchport mode trunk – **создаем trunk интерфейс в сторону роутера**;

SW1 (config-if)# switchport trunk encapsulation dot1q – **назначаем ему инкапсуляцию**;

SW1 (config-if)# switchport trunk allowed vlan 1-2,3,1002-1005 – **определяем, какие vlan-ы будут пропускаться в trunk (по желанию)**;

SW1 (config-if)# exit

SW1 (config)# exit

SW1# wr

Коммутатор SW2:

R2>en

R2#conf t

R2(config)# hostname SW2

R2(config)# exit

SW2# vlan database

SW2 (vlan)# vlan 4 name PERSONAL

SW2 (vlan)# exitSW2# conf t

SW2 (config)#int fa range 0/2-8

SW2 (config-if)#switchport mode access

SW2 (config-if)#switchport access vlan 4

SW2 (config-if)#exit

SW2 (config)#int fa range 0/11-12

SW2 (config-if)#switchport mode access

SW2 (config-if)#switchport access vlan 4

SW2 (config-if)#exit

SW2 (config)#int fa 0/14

SW2 (config-if)#switchport mode access

SW2 (config-if)#switchport access vlan 4

SW2 (config-if)#exit

SW2 (config)#int fa 1/15

SW2 (config-if)# switchport mode trunk

SW2 (config-if)# switchport trunk encapsulation dot1q

SW2 (config-if)# switchport trunk allowed vlan 1-2,1002-1005

SW2 (config-if)#exit

SW2 (config)#exit

SW2# wr

Теперь перейдем к настройке роутера :

R1>en

R1# conf t

R1(config)# hostname sanek

sanek (config)# int loopback 0 – **создаем loopback интерфейс**;

sanek (config-if)# ip address 10.10.10.10 255.255.255.255 –**задаем ему IP-адрес**;

sanek (config-if)#exit

sanek (config)# int fa 0/0

sanek (config-if)# no shutdown

sanek (config-if)# exit

sanek (config)# int fa 0/0.2 – **создаем sub-интерфейсы для ранее созданных vlan-ов и назначаем им соответствующие IP-адреса**;

sanek (config-subif)# encapsulation dot1Q 2

sanek (config-subif)# ip address 192.168.1.1 255.255.255.0

sanek (config-subif)# ip nat inside – **указываем, что данный интерфейс будет использоваться для NAT**;

sanek (config-subif)# exit

sanek (config)# int fa 0/0.3

sanek (config-subif)# encapsulation dot1Q 3

sanek (config-subif)# ip address 192.168.2.1 255.255.255.0

sanek (config-subif)# ip nat inside

sanek (config-subif)# exit

sanek (config)# int fa 1/0

sanek (config-if)# ip address 1.1.1.1 255.255.255.252 – **назначаем IP-адрес на интерфейсе, смотрящем в сторону интернета**;

sanek (config-if)# no shutdown

sanek (config-if)# ip nat outside – **определяем его как выходной интерфейс для NAT**;

sanek (config-if)# exit

sanek (config)#int tunnel 0 – **создаем интерфейс для GRE туннеля**;

sanek (config-if)# ip address 172.16.1.1 255.255.255.0 –**назначаем ему IP-адрес**;

sanek (config-if)# tunnel source fa 1/0 – **определяем «начало» GRE туннеля**;

sanek (config-if)# tunnel destination 2.2.2.1 – **определяем «конец» GRE туннеля**;

sanek (config-if)# exit

sanek (config)# ip access-list extended For_NAT – **создаем список доступа и определяем какие сети попадают под NAT**;

sanek (config-ext-nacl)# permit ip 192.168.1.0 0.0.0.255 any

sanek (config-ext-nacl)# permit ip 192.168.2.0 0.0.0.255 any

sanek (config-ext-nacl)# exit

sanek (config)# ip nat inside source list For_NAT interface fa 1/0 overload – **включаем NAT на роутере**;

sanek (config)# ip route 0.0.0.0 0.0.0.0 1.1.1.2 – **прописываем маршрут по умолчанию**;

sanek (config)# ip route 192.168.3.0 255.255.255.0 tunnel 0 – **прописываем маршрут в удаленную сеть через туннель GRE**;

sanek (config)# exit

sanek # wr

Теперь приступим к настройке VoIP. Заходим на роутер и добавляем следующую конфигурацию:

sanek >en

sanek #conf t

sanek (config)# telephony-service – **заходим в режим настройки телефонных сервисов**;

sanek (config-telephony)# max-ephones 10 – **назначаем максимальное количество IP-телефонов, которое нам потребуется в нашей «телефонной» сети;**

sanek (config-telephony)# max-dn 10 **– назначаем максимальное количество «телефонных» линий**;

sanek (config-telephony)#ip source-address 10.10.10.10 port 2000 – **задаем IP-адрес и порт (port 2000 – порт по умолчанию), на который будут обращаться IP-телефоны для регистрации**;

sanek (config-telephony)#exit

sanek (config)#voice service voip – **заходим в режим конфигурации голосового сервиса для задания инкапсуляции Voice over IP**;

sanek (conf-voi-serv)#allow-connections h323 to h323 – **включаем звонки между соответствующими типами конечных точек**;

sanek (conf-voi-serv)#allow-connections h323 to sip

sanek (conf-voi-serv)#allow-connections sip to sip

sanek (conf-voi-serv)#allow-connections sip to h323

sanek (conf-serv-sip)#exit

sanek (config)#voice class codec 1 – **создадим список поддерживаемых кодеков**;

sanek (config-class)#codec preference 1 g711ulaw – **указываем, в каком порядке какой кодек применять**;

sanek (config-class)#codec preference 2 g711alaw

sanek (config-class)#codec preference 3 g729r8

sanek (config-class)#exit

sanek (config)#ephone-dn 1 – **создаем первую логическую «телефонную» линию (directory number). Каждому телефону можно определить несколько таких логический линий со своими номерами**;

sanek (config-ephone-dn)#number 1001 – **задаем номер, который будет соответствовать этой линии**;

sanek (config-ephone-dn)#name Host_A – **задаем имя, которое будет отображаться при звонке на IP-телефоне**;

sanek (config-ephone-dn)#exit

sanek (config)#ephone-dn 2

sanek (config-ephone-dn)#name Host_A

sanek (config-ephone-dn)#number 2001

sanek (config-ephone-dn)#name Host_B

sanek (config-ephone-dn)#exit

sanek (config)#ephone 1 – **создаем первый IP-телефон**;

sanek (config-ephone)#mac-address 0800.279D.D0F4 – **задаем ему mac-address. Он будет использоваться в качестве уникального имени IP-телефона. Взять его можно из установок вашей сетевой карты на компьютере**;

sanek (config-ephone)#type cipc – **указываем тип IP-телефона. В нашем случае – это Cisco IP Communicator**;

sanek (config-ephone)#button 1:1 – **указываем IP-телефону, что первая клавиша на нем, будет соответствовать первой логической линии (directory number)**;

sanek (config-ephone)#exit

sanek (config)#ephone 2

sanek (config-ephone)#mac-address 0800.277E.9718

sanek (config-ephone)#type cipc

sanek (config-ephone)#button 1:2

sanek (config-ephone)#exit

sanek (config)#dial-peer voice 1 voip – **для создания связи с удаленным офисом нам необходимо настроить соседство между CME. Заходим в соответствующий режим**;

sanek (config-dial-peer)#destination-pattern 30.. – **указываем, что если кто то набирает номер, начинающийся на «30», то отправлять его на соседний CME**;

sanek (config-dial-peer)#session target ipv4:20.20.20.20 –**прописываем, что телефонная сессия должна быть установлена через IP сеть и адрес удаленного CME 20.20.20.20**;

sanek (config-dial-peer)#voice-class codec 1 – **указываем, какие кодеки могут быть использованы для данной связи**;

sanek (config-dial-peer)#exit

sanek # wr

ГЛАВА 4. ОХРАНА ТРУДА

4.1.Законы об охране труда республики Узбекистан

Этот раздел дипломной работы посвящён рассмотрению воздействия опасных и вредных производственных факторов, действующих на оператора персональной ЭВМ, а также методы, позволяющие снизить уровень их влияния.

Законодательство об охране труда состоит из настоящего Закона и издаваемых в соответствии с ним других нормативных актов.

Действие настоящего Закона распространяется на всех работников, состоящих в трудовых отношениях с предприятиями, учреждениями, организациями различных форм собственности и хозяйствования, в том числе с отдельными нанимателями; членов кооперативов, студентов высших учебных заведений, учащихся средних специальных учебных заведений, профессионально-технических училищ и общеобразовательных школ, проходящих производственную практику; военнослужащих, привлекаемых для работы на предприятиях; граждан, проходящих альтернативную службу; лиц отбывающих наказание по приговору суда, в период их работы на предприятиях исправительно-трудовых учреждений или предприятиях, определяемых органами, ведающими исполнением приговоров, а также на участников других видов трудовой деятельности, организуемой в интересах общества и государства.

Таких психологических факторов, как умственное перенапряжение, перенапряжение слуховых и зрительных анализаторов, монотонность труда, эмоциональные перегрузки. Не последнее место в работе оператора занимает и эргономика его рабочего места, которая включает в себя кроме перечисленных факторов требования к комфортности самого рабочего места, одежде и др.

Длительное нахождение человека в зоне одновременного воздействия различных неблагоприятных факторов может привести к профессиональному заболеванию. Анализ травматизма среди операторов ЭВМ показывает, что в основном несчастные случаи происходят при выполнении ими несвойственным им работ. На втором месте несчастные случаи, связанные с воздействием электрического тока. Мера воздействия большинства вредных производственных факторов, которые испытывает оператор, работающий на персональной ЭВМ, нормируются. В данном разделе приведены фактические значения опасных и вредных факторов, создаваемых на рабочем месте оператора, а также допускаемые нормативные значения данных факторов.

4.2 Анализ опасных и вредных факторов

Электрические установки, к которым относится практически всё оборудование ЭВМ, представляют для человека потенциальную опасность. Несмотря на то, что источник питания модулей микроЭВМ имеет низкое (5 [В]) и, следовательно, безопасное напряжение, это не исключает возможности поражения оператора электрическим током. Наличие в блоке питания силового трансформатора, первичная обмотка которого подключена к напряжению 220 [В], а также использование электрифицированных инструментов и измерительных приборов, питающимися от сети 220 [В], создают дополнительную опасность электротравматизма.

Для предотвращения поражения операторов ЭВМ электрическим током исключительно важная роль отводится правильной организации обслуживания действующих электроустановок, проведению превентивных профилактических работ по технике безопасности. При этом под правильной организацией работ понимается строгое выполнение ряда организационных и технических мероприятий и средств, установленных действующими «Правилами технической эксплуатации электроустановок потребителей и правила техники безопасности при эксплуатации электроустановок потребителей» и «Правила установки электроустановок» (ПУЭ).

Необходимо также отметить, что все современные ЭВМ соответствуют общепринятым международным стандартам на уровень защищённости электроприборов, что сводит риск поражения электрическим током при работе с ними к минимуму.

4.2.1 Повышенный уровень электромагнитных излучений

Источником интенсивных электромагнитных полей инфранизких частот является как монитор ЭВМ так и системный блок. У большинства мониторов создаваемые ими электромагнитные поля значительно сильнее по бокам и сзади, чем перед самим экраном. В 1999 г. был принят новый ряд международных стандартов, на уровень электромагнитного излучения мониторов. Поэтому помещение оснащается мониторами, поддерживающими стандарт ТСО 99. В противном случае следует оснастить мониторы ЭВМ стеклянными защитными фильтрами, которые необходимо обязательно заземлить.

Согласно действующим строительным нормам и правилам СНиП 11-4-79 для естественного освещения регламентирован коэффициент естественной освещенности КЕО. При этом наименьшим объектом различения является точка на экране монитора. Определим размер точки исходя из того, что разрешение пятнадцатидюймового монитора с адаптером SVGA, работающего при экранном разрешении 1024x768 точек. При этом размер экрана 320x210 мм, следовательно, наименьший размер объекта различения - минимальный из двух значений: 210 / 768 = 0.27 мм; 320/1024 = 0.31 мм, то есть 0.27 мм.

4.3 Санитарно гигиенические требования к операторам на рабочем месте

Согласно действующим строительным нормам и правилам СНиП 11-4-79 для искусственного освещения регламентирована наименьшая допустимая освещенность рабочих мест.

Рекомендуемая освещенность для работы с экраном дисплея составляет 200 [лк], а при работе с экраном в сочетании с работой над документами – 400 [лк].

Для искусственного освещения помещения узла применяются люминесцентные лампы ЛТБ (тепло-белый свет) мощностью 40 Вт, у которых высокая световая отдача, продолжительный срок службы, малая яркость светящейся поверхности и спектральный состав близкий к естественному.

Система общего искусственного освещения выполнена потолочными лампами, размещенными параллельно светопроёмам и равномерно по потолку.

Чтобы избежать отражений, которые могут снизить четкость восприятия, не следует располагать рабочее место прямо под источником света. Основными источниками шума при работе с ЭВМ являются электродвигатели охлаждающего вентилятора блока питания ЭВМ, принтеры, использующие механические способы печати (матричные принтеры), работающие накопители на гибких магнитных дисках (дисководы) а также работающая офисная техника (ксероксы, сканеры). Первые источники шума относят к постоянным, остальные к импульсным.

Как правило, уровень шума в современных условиях не превышает допустимого уровня. Для предотвращения электрического травматизма необходимо:

1. Обеспечить правильную организацию обслуживания действующих электрических установок, установленную "Правилами технической эксплуатации электроустановок потребителей" (ПТЭ) и "Правилами устройства электроустановок" (ПУЭ).

2. Обеспечить надёжную электрическую изоляцию токоведущих частей.

3. Обеспечить все электроприборы защитным заземлением (3-х полюсные вилки и розетки).

В качестве таких мероприятий рекомендовано:

1. Экранирование дисплея (источника ЭМП). В стекло ЭЛТ добавляется оксид свинца, либо используется защитный оптический экран (optical glass filter) .

2. Удаление рабочего места от источника ЭМП. Пользователям, желающим снизить уровень облучения, следует расположиться так, чтобы расстояние до экрана монитора составляло величину, равную длине вытянутой руки.

3. Рациональное размещение оборудования. Предусмотрено расположение на расстоянии не менее 1.22 [м] от боковых и задних стенок других мониторов. Оператор располагается на расстоянии 50-70 [см] от экрана монитора.

4. Защита временем. Допустимое время пребывания за экраном монитора T, ч : $T = 50/E–2$, где E – напряженность электрической составляющей воздействующего поля в зоне монитора, [кВ/м]. При E = 8,5 [кВ/м] : $T = 50/8,5 = 3,8$ [ч]. Таким образом, необходимо проводить за монитором не более 4 часов в сутки и не более 20 часов в неделю.

5. Использование новых видов техники. Любой монитор, работающий на не ЭЛТ, не излучает переменных ЭМП, связанных с наличием систем вертикального и горизонтального отклонения электронного луча. Такими мониторами являются жидкокристаллические дисплеи (LCD), которые рекомендованы для замены имеющихся. Дополнительное достоинство таких дисплеев – это также то, что оператор видит полученное на них изображение не в прямом, а в отражённом свете, что снижает утомляемость глаз.

Для обеспечения надлежащего качественного (в т.ч. аэроионного и непыльного) состава воздуха предусмотрены:

1. Систематические проветривание помещений.

2. Ежедневная влажная уборка.

3. Поддержка работоспособности приточно-вытяжной вентиляции.

4. Установка автономных кондиционеров в оконных рамах, число которых определяется согласно расчету воздухообмена и по количеству теплоизбытка от ЭВМ, числа работающего персонала и солнечной радиации.

Для исключения дестабилизирующего микроклимат (и освещение) влияния солнечной радиации на окнах обязательно наличие жалюзи.

Для обеспечения пожарной безопасности используют организационные, эксплуатационные, технические и режимные мероприятия по противопожарной защите.

Организационные мероприятия предусматривают правильную эксплуатацию оборудования, правильное содержание помещений, наличие огнетушащих средств, наличие пожарной сигнализации, противопожарный инструктаж обслуживающего персонала.

К техническим мероприятиям относятся: соблюдение противопожарных правил, норм при устройстве электрических проводок и электрооборудования, правильное размещение оборудования.

Мероприятия режимного характера – это, как правило, запрещение курения в неположенных местах, производство сварочных и других работ в пожароопасных помещениях.

Эксплуатационными мероприятиями являются своевременные профилактические осмотры, ремонты и испытания технологического оборудования.

Любая современная ПЭВМ (за исключением переносных компьютеров работающих от источников питания в 5[В]), является прежде всего электроприбором, подключённым к сети в 220[В]. И хотя ЭВМ и рассчитаны на безопасную постоянную работу, всё же возможны случаи, когда некачественная сборка блока питания, может привести к короткому замыканию, которое может привести к возгоранию. Кроме того напряжение к электроустановкам подается по кабельным линиям, которые также представляют особую пожарную опасность.

ЗАКЛЮЧЕНИЕ

В этой выпускной работе была исследования локальная сеть Ethernet для рабочих мест в учреждении. Данная сеть позволяет подключить 14 рабочих станции. Сеть предусматривает взаимодействие с сетью Token Ring. Обеспечивается передача данных со скоростью 10 Мбит/с. В данном проекте были изучены принципы построения сетей, изучена архитектура сети Ethernet, подобрано сетевое оборудование и сервер, спроектирована структурированная кабельная система. Данная кабельная система обладает максимальной гибкостью, возможностью внедрения новых технологий, возможностью подключения различных видов оборудования. Также был произведён расчёт длин кабеля и мощности устанавливаемого источника бесперебойного питания. Показана физическая и логическая схема сети. Спроектированная сеть соответствует установленным требованиям и стандартам и является высокопроизводительной и надёжной сетью. Рассчитана смета всего оборудования и стоимость монтажных работ. Было дано экономическое обоснование проекта и рассчитана смета затрат на проектирование сети. Была произведена оценка стоимости монтажных работ. Подобрано программное обеспечение, устанавливаемое на рабочие станции. Так же подобраны камеры видеонаблюдения как для улицы так и внутренние камеры устанавливаемые в образовательное учреждение. Показана установка и настройка SQUID и DCHP на Ubuntu Server 10.10. Так же выбран провайдер для сети образовательного учреждения и поставщик оборудования. Сделан полный обзор сетевых кабелей и кабель - каналов. Подобрано программное обеспечение для сервера, а так же и для персональных компьютеров установленных у образовательном учреждении. По всему образовательному учреждению установлены видео камеры, вся запись с видеонаблюдения сохраняется на сервере.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1.Аппаратные средства локальной сети. Энциклопедия. Кварцов И.Я. 2005г. (http://knowledge.allbest.ru/radio/3c0b65625b3ad78b5d53a89521306c36_0.html)

2.Компьютерные сети. Модернизация и поиск неисправностей. Пер. с англ. Джордан Валлос 2006г. (http://www.vevivi.ru/best/Proektirovanie-lokalnoi-seti-ref193845.html)

3.Современные компьютерные сети. Моргунов Ж.Ц. 2008г. (http://knowledge.allbest.ru/programming/2c0b65625a3bc68b5c43a88421316c27_0.html)

4.Компьютерные сети. Принципы, технологии, протоколы. Акропов П.Ц. 2006г. (http://www.bibliofond.ru/view.aspx?id=446061)

5.Компьютерные сети, протоколы и технологии интернета. (http://csspinfo.ru/kompyuternye-seti-protokoly-i-tehnologii-interneta.html)

6. Иваницкий К.А., Печников В.Н. ALT Linux с нуля! Школьная операционная система (+ DVD-ROM) - Издательство: Лучшие Книги, 2009

7. Колисниченко Д.Н., Аллен Питер В. LINUX: полное руководство. — СПб: Наука и Техника, 2006

8. Костромин В.А. Основы работы в ОС Linux. Курс ИНТУИТ.ру. - www.intuit.ru

9. Костромин В.А., Разделы диска и средства для работы с ними в Линукс. - http://www.linuxcenter.ru/lib/books/partitioning/

10.Корнеев Д. Права доступа к файлам в Linux - http://old.linux.kiev.ua/modules.php?name=News&file=article&sid=703

11. Кузнецов С.В. - История создания UNIX - http://www.linuxcenter.ru/lib/history/unix_gentree.phtml

12. Маслинский К. Операционная система Linux - ИНТУИТ.ру, 2005.

13. Маслинский К., Отставнов М. «Графический интерфейс в Linux» -