МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Кафедра Компьютерных технологий

«Допущен к защите»
Заведующий кафедрой
Куралбаев З.К., д.ф.-м.н., проф.
(Ф.И.О., ученая степень, звание)
_____ «_____»_____**20__ г.**
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Разработка комплекса лабораторных работ по дисциплине «Компьютерные сети
Специальность: 5В070400 – Вычислительная техника и программное обеспечение

Выполнил: Искаков Б.С. **группа:** ВТ 12-2

Научный руководитель: Тергеусизова А.С., старший преподаватель

Консультанты:

по экономической части:
Бекишева А.И., к. э. н., доцент
_____ «12» 05 2016 г.
(подпись)

по безопасности жизнедеятельности:
Мазалов И.Ф., к. х. н., доцент
_____ «11» 05 2016 г.
(подпись)

по применению вычислительной техники:
Тергеусизова А.С., старший преподаватель
_____ «30» 05 2016 г.
(подпись)

Нормоконтролер: Тергеусизова А.С., старший преподаватель
_____ «30» 05 2016 г.
(подпись)

Рецензент: Аманбаев Е.А. АО Сбербанк, главный риск менеджер
(Фамилия и инициалы, ученая степень, звание)
_____ «30» мая 2016 г.
(подпись)

Алматы 2016 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Факультет: Аэрокосмических и информационных технолоий
Специальность: 5В070400 – Вычислительная техника и программное обеспечение
Кафедра: Компьютерных технологий

ЗАДАНИЕ
на выполнение дипломного проекта

Студент: Искаков Б.

Тема проекта: «Разработка комплекса лабораторных работ по дисциплине «Компьютерные сети»», утверждена приказом ректора № 148 от «19» октября 2015 г.

Срок сдачи законченной работы «20» мая 2016г.

Исходные данные к проекту требуемые параметры результатов проектирования (исследования) и исходные данные объекта

Разработать 8 лабораторных работ по дисциплине «Компьютерные сети», в соответствии с рабочей программой дисциплины и следующих порядку лекционного материала. Необходимо собрать лабораторный стенд с использованием оборудования компании Cisco systems и дать практические рекомендации, порядок выполнения лабораторных работ.

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

1. Комплекс лабораторных работ
2. Разработка системы обучения
3. Компьютерные сети
4. Сетевые технологии: коммутация и маршрутизация в сетях
5. Коммутируемые сети без границ
6. Маршрутизация
7. Методические указания

Перечень графического материала (с точным указанием обязательных чертежей)

1. Топология сети – Знакомство с учебным стендом
2. Топология сети – Первоначальная настройка сетевых устройств
3. Топология сети – Администрирование коммутаторов
4. Топология сети – Конфигурирование портов и работа с таблицей коммутации
5. Топология сети – Виртуальные локальные сети VLAN
6. Топология сети – Маршрутизация между VLAN
7. Топология сети – Статическая маршрутизация
8. Топология сети – Протокол маршрутизации RIPv2

Рекомендуемая основная литература

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник. – Санкт–Петербург: Питер, 2012г.
2. Тойгожинова А.Ж., Тергеусизова А.С. Компьютерные сети: Конспект лекций. – Алматы:АУЭС, 2014г.
3. Майкл В. Маршрутизаторы CISCO для отчаявшихся администраторов. Простые методы управления маршрутизаторами и коммутатотарами: Учебник. - Cisco press, 2010г.
4. В.П. Шувалов. Телекоммуникационные системы и сети. - Горячая линия: Телеком, 2012г.
5. М. А. Ташимов. Технологии коммуникационных компьютерных сетей. - Алматы: ТОО Print-S, 2008г.

Консультанты по проекту с указанием относящихся к ним разделов

Раздел	Консультант	Сроки	Подпись
Основная часть	Тергеусизова а.С.	30.03 – 17.05	
Безопасность жизнедеятельности	Мазалов И.Ф.	11.03 – 11.05.16	
Экономическая часть	Бекишева А.И.	30.03 – 2.05.16	
Нормоконтролер	Тергеусизова А.С.	30.03 – 30.05.16	
Прим.выч.техн.	Тергеусизова А.С.	30.03 – 30.05.16	

Г Р А Ф И К
подготовки дипломного проекта

№ п/п	Наименование разделов, перечень разрабатываемых вопросов	Сроки представления руководителю	Примечание
1.	Комплекс лабораторных работ	01.03-08.03	
2.	Разработка системы обучения	08.03 – 15.03	
3.	Компьютерные сети	15.03 – 28.03	
4.	Сетевые технологии: коммутация и маршрутизация в сетях	15.03 – 27.03	
5.	Коммутируемые сети без границ	28.03 – 16.04	
6.	Маршрутизация	28.03 – 16.04	
7.	Методические указания (Лабораторные работы 1,2,3)	16.04 – 24.05	
8.	Методические указания (Лабораторные работы 4,5,6)	16.04 – 24.05	
9.	Методические указания (Лабораторные работы 7,8)	16.04 – 24.05	

Дата выдачи задания «14» октября 2015 г.

Заведующий кафедрой _____ Куралбаев З.К.
(подпись)

Руководитель _____ Тергеусизова А.С.
(подпись)

Задание принял к исполнению
студент _____ Искаков Б.
(подпись)

Аннотация

Дипломная работа посвящена разработке комплекса лабораторных работ по дисциплине «Компьютерные сети». Лабораторные работы основаны на современных методах коммутации и маршрутизации данных. Комплекс состоит из четырех лабораторных работ, с указанием рабочего задания, методических указаний, порядка выполнения и контрольных вопросов.

Аңдатпа

Бұл диплодық жұмыс «Компьютерлік желілер» пәні бойынша зертханалық жұмыстардың жиынтығын өңдеуге арналады. Зертханалық жұмыс желілік жабдықтардың арқасында ақпараттық қауіпсіздіктің заманауи әдістеріне негізделген. Жиынтық төрт зертханалық жұмыстан тұрады, жұмыстық тапсырманың нұсқаулығынан, әдістемелік нұсқаудан, орындау тәртібінен және тексеру сұрақтарынан.

Abstract

The thesis is devoted to development of a complex of laboratory works on discipline "C omputer networks ". Laboratory works are based on modern methods of information security with use of the network equipment. The complex consists of four laboratory works, with the indication of a working task, methodical instructions, an order of performance and control questions.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Вопрос безопасности всегда стоял перед компьютерными сетями, но сегодня как никогда растет осознание того, насколько важна безопасность компьютерных сетей в корпоративных инфраструктурах.

Сетевая безопасность (анг. Network Security) - это набор требований, предъявляемых к инфраструктуре компьютерной сети предприятии и политикам работы в ней, при выполнении которых обеспечивается защита сетевых ресурсов от несанкционированного доступа.

Основные принципы сетевой безопасности:

- защита внутренних сетей от несанкционированного доступа;
- обеспечение безопасного подключения к сети Интернет и безопасного удаленного доступа;
- контроль за работой различных онлайн-приложений, через которые также возможен доступ к персональным компьютерам.
- предоставление возможности осуществления коммерческих операций через Интернет.

Дипломный проект направлен на разработку комплекса лабораторных работ и представляет собой разработку системы обучения студентов в области безопасности компьютерных сетей.

Лабораторные работы предназначены для знакомства студентов с системами безопасности в области компьютерных сетей и приобретению навыков работы с современным оборудованием обеспечивающим безопасность ИТ - инфраструктуры.

Разработанный комплекс лабораторных работ отличается следующими особенностями:

- обучение на базе самого современного оборудования;
- углубленное изучение вопросов обеспечения безопасности КС;
- создание защищенных сетей;
- повышение качества знаний и уровня квалификации студентов.

В комплекс включен весь спектр работ, необходимый для получения основных навыков при конфигурации, настройки и реализации систем защиты.

ГЛАВА 1 КОМПЛЕКС ЛАБОРАТОРНЫХ РАБОТ

1.1 Разработка системы обучения

Современный мир динамичен и изменчив: компании выбирают всё более эффективные методы ведения ежедневного бизнеса, и одновременно с этим непрерывно совершенствуются сетевые технологии. В наши дни пользователи рассчитывают на получение прямого доступа к ресурсам компании — в любое время и из любой точки мира. Под этими ресурсами подразумеваются не только традиционные виды данных, но также видео и голосовая информация. Наряду с этим возрастает потребность в средствах организации коллективной работы, позволяющих в реальном времени осуществлять обмен ресурсами между множеством удалённых сотрудников, как если бы они находились в одном офисе.

Различные устройства должны органично взаимодействовать друг с другом для обеспечения быстрого, безопасного и надёжного соединения между узлами. Коммутаторы локальных сетей обеспечивают подключение конечных пользователей к корпоративной сети и, главным образом, отвечают за управление информацией внутри среды LAN. Маршрутизаторы обеспечивают передачу информации между сетями LAN и, как правило, не взаимодействуют с отдельными узлами. Все современные сервисы зависят от доступности надёжной маршрутизируемой и коммутируемой сетевой инфраструктуры, на основе которой они могут быть построены. Данная инфраструктура должна быть тщательно разработана, правильно развёрнута и организована для обеспечения стабильности платформы.

С этой главы мы начнём изучение понятия потока трафика в современной сети. В главе также рассматриваются некоторые современные модели проектирования сетей и способы построения коммутаторами локальной сети таблиц пересылки и использования информации о MAC-адресах для эффективной передачи данных между узлами.

Для обеспечения максимальной доступности, гибкости, безопасности и удобства эксплуатации коммутируемой сети без границ в процессе её создания необходимо следовать чётким принципам проектирования. Коммутируемая сеть без границ должна соответствовать текущим и возможным будущим требованиям к работе сервисов и технологий. Руководство по проектированию коммутируемой сети без границ построено на принципах, перечисленных ниже.

Иерархичность упрощает понимание роли каждого устройства на каждом уровне, обеспечивает поддержку в процессе развёртывания, эксплуатации и управления, а также снижает количество неполадок на каждом уровне.

Модульность способствует безупречному расширению сети и внедрению интегрированных сервисов по мере необходимости.

Отказоустойчивость обеспечивает бесперебойную работу сети в соответствии с ожиданиями пользователей.

Гибкость обеспечивает рациональное распределение нагрузки трафика за счёт использования всех сетевых ресурсов.

Перечисленные принципы зависят друг от друга. Именно поэтому крайне важно понимать природу и способы их взаимодействия в рамках коммутируемой сети. Иерархическое проектирование коммутируемой сети без границ (рисунок 1.1) создаёт основу, которая позволяет сетевым разработчикам объединять функции безопасности, мобильности и унифицированной коммуникации. Три основных уровня в рамках рассматриваемых многоуровневых проектов представляют собой уровни доступа, распределения и ядра. Каждый уровень можно рассматривать как чёткий, структурированный модуль кампусной сети, наделённый определёнными ролями и функциями. Введение принципа модульности в иерархическую архитектуру сети даёт дополнительную гарантию — кампусные сети модульных конструкций демонстрируют большую надёжность и гибкость в отношении обеспечения важнейших сетевых сервисов.

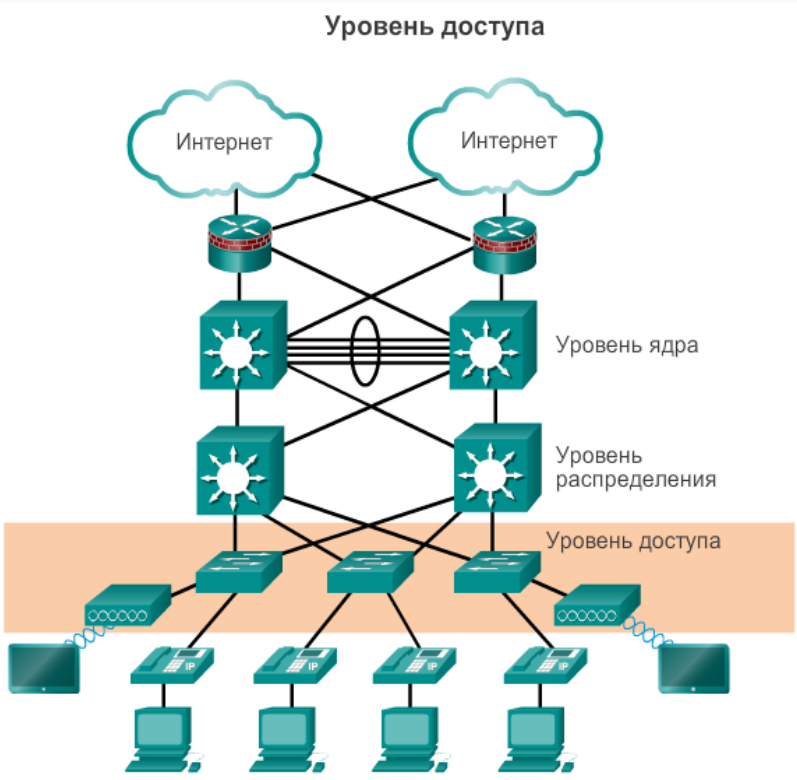

Рисунок 1.1 – Проект иерархической сети

За последние два десятилетия роль коммутируемых сетей существенно возросла. Совсем недавно повсеместно использовались плоские коммутируемые сети 2-го уровня. Для передачи трафика LAN в рамках организации плоские сети передачи данных 2-го уровня полагались на базовые свойства стандарта Ethernet и широкое использование повторителей и концентратора. В иерархической топологии произошла радикальная замена сетей на коммутируемые LAN. Коммутируемая LAN обеспечивает большую гибкость, оптимизированное управление трафиком и следующие дополнительные функции:

- качество обслуживания;
- дополнительная безопасность;
- поддержка беспроводных сетей и подключения;
- поддержка таких новых технологий, как IP-телефония и мобильных сервисов. Пример топологии коммутируемых сетей приведен на рисунке 1.2.

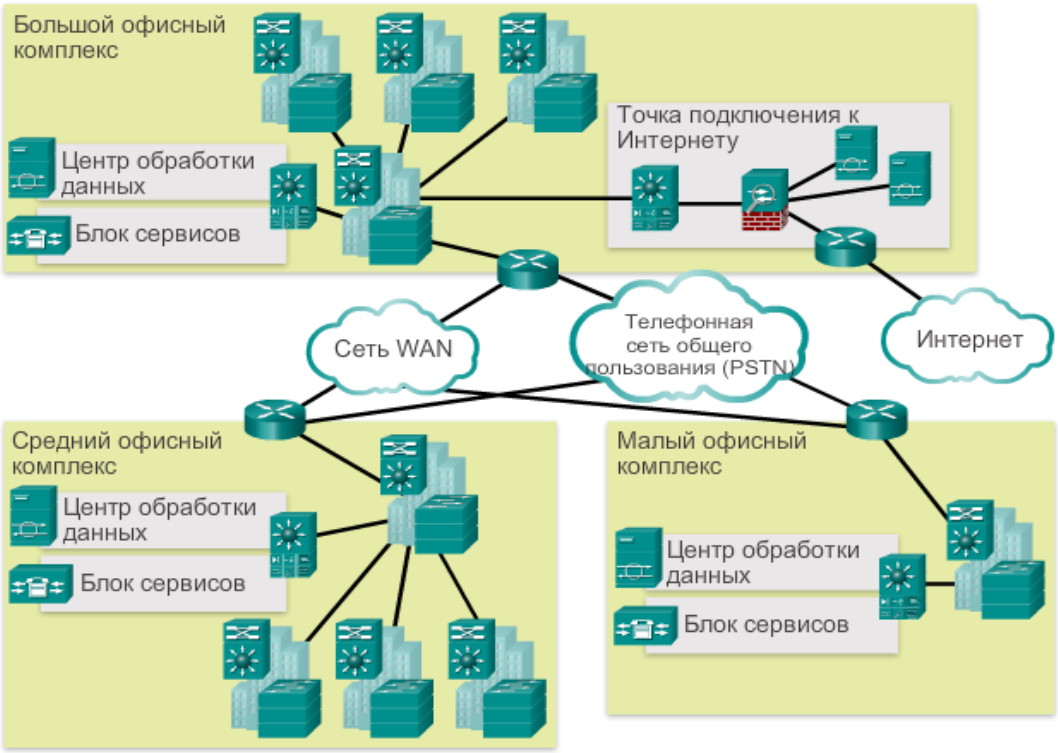

Рисунок 1.2 – Коммутируемые сети без границ

Архитектура виртуальных локальных сетей

Производительность сети является важным фактором эффективности работы организации. Одной из технологий повышения производительности сети является разделение крупных широковещательных доменов на более мелкие. Маршрутизаторы устроены таким образом, что блокируют широковещательный трафик на интерфейсе. При этом маршрутизаторы обычно имеют ограниченное количество интерфейсов LAN. Основная роль маршрутизатора заключается в передаче информации между сетями, а не в предоставлении оконечные устройства доступа к сети.

Предоставление доступа в локальную сеть обычно обеспечивается коммутатором уровня доступа. Для уменьшения размера широковещательных доменов на коммутаторе 2-го уровня, как и на устройстве 3-го уровня, можно создать сеть VLAN. Сети VLAN обычно включаются в проекты сети, для того чтобы сеть облегчала процесс достижения целей организации. Несмотря на то что сети VLAN в основном используются в коммутируемых локальных сетях, современные реализации VLAN способны функционировать также в муниципальных (MAN) и глобальных (WAN) сетях.

Определение виртуальной локальной сети

В коммутируемых объединённых сетях сети VLAN обеспечивают гибкость сегментации и организации. Сети VLAN позволяют сгруппировать устройства внутри локальной сети. Группа устройств в пределах сети VLAN взаимодействует так, будто устройства подключены с помощью одного провода. Сети VLAN основываются не на физических, а на логических подключениях (рисунок 1.3).

Сети VLAN позволяют администратору производить сегментацию по функциям, проектным группам или областям применения, вне зависимости от физического расположения пользователя или устройства. Устройства в пределах сети VLAN работают таким образом, будто находятся в собственной независимой сети, даже если делят одну общую инфраструктуру с другими VLAN. Любой порт коммутатора может принадлежать сети VLAN. Одноадресные, широковещательные и многоадресные пакеты пересылаются и рассылаются только к конечным станциям в пределах той сети VLAN, которая является источником этих пакетов. Каждая сеть VLAN считается отдельной логической сетью, и пакеты, адресованные станциям, не принадлежащим данной сети VLAN, должны пересылаться через устройство, поддерживающее маршрутизацию.

Сеть VLAN создаёт логический широковещательный домен, который может охватывать несколько физических сегментов LAN. Разделяя крупные широковещательные домены на более мелкие сети, VLAN повышают производительность сети. Если устройство в одной сети VLAN передаёт широковещательный кадр Ethernet, то этот кадр получают все устройства в рамках этой VLAN, устройства же в других сетях VLAN этот кадр не получают.

Сети VLAN позволяют реализовывать политику обеспечения доступа и безопасности, учитывая интересы различных групп пользователей. Каждый порт коммутатора может быть назначен только одной сети VLAN (за исключением порта, подключённого к IP-телефону или к другому коммутатору).

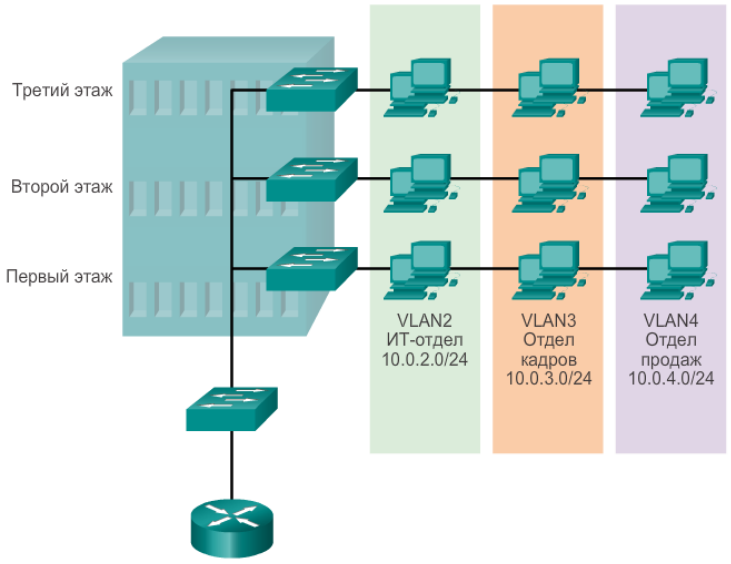

Рисунок 1.3 – Определение групп виртуальной локальной сети (VLAN)

Преимущества виртуальных локальных сетей (VLAN).

Производительность пользователей и адаптивность сети играют важную роль в процветании и успехе компании. Сети VLAN облегчают процесс проектирования сети, обеспечивающей помощь в выполнении целей организации. К основным преимуществам использования VLAN относятся:

1) Безопасность: группы, обладающие уязвимыми данными, отделены от остальной части сети, благодаря чему снижается вероятность утечки конфиденциальной информации. Как показано на рисунке, компьютеры преподавателей находятся в сети VLAN 10 и полностью отделены от трафика данных учащихся и гостей.

2) Снижение расходов: благодаря экономии на дорогих обновлениях сетевой инфраструктуры и более эффективному использованию имеющейся полосы пропускания и восходящих каналов происходит снижение расходов.

3) Повышение производительности: разделение однородных сетей 2-го уровня на несколько логических рабочих групп (широковещательных доменов) уменьшает количество лишнего сетевого трафика и повышает производительность.

4) Уменьшенные широковещательные домены: разделение сети на сети VLAN уменьшает количество устройств в широковещательном домене. Сеть, показанная на рисунке, состоит из шести компьютеров и трёх широковещательных доменов: для преподавателей, для учащихся и гостевого домена.

5) Повышение производительности ИТ-отдела: сети VLAN упрощают управление сетью, поскольку пользователи с аналогичными требованиями к сети используют одну и ту же сеть VLAN. При введении в эксплуатацию нового коммутатора на назначенных портах реализуются все правила и процедуры, уже применённые в этой конкретной VLAN. Также ИТ-специалистам легче определять функцию сети VLAN, назначая ей соответствующее имя. На данном рисунке для простой идентификации сеть VLAN 10 была названа «Для преподавателей», VLAN 20 — «Для учащихся» и VLAN 30 — «Гостевая».

6) Упрощённое управление проектами и приложениями: сети VLAN объединяют пользователей и сетевые устройства для соответствия деловым или географическим требованиям сети. Управление проектом и работа на прикладном уровне упрощены благодаря использованию разделения функций. Пример такой прикладной задачи — платформа разработки приложений для электронного обучения преподавателей.

Каждая VLAN в коммутируемой сети относится к какой-либо IP-сети; таким образом, в проекте VLAN нужно учитывать реализацию иерархической системы сетевой адресации. Иерархическая адресация подразумевает упорядоченное назначение номеров IP-сети сегментам или сетям VLAN с учетом работы сети в целом. Как показано на рисунке 1.4, блоки смежных сетевых адресов резервируются и настраиваются на устройствах в определённой области сети.

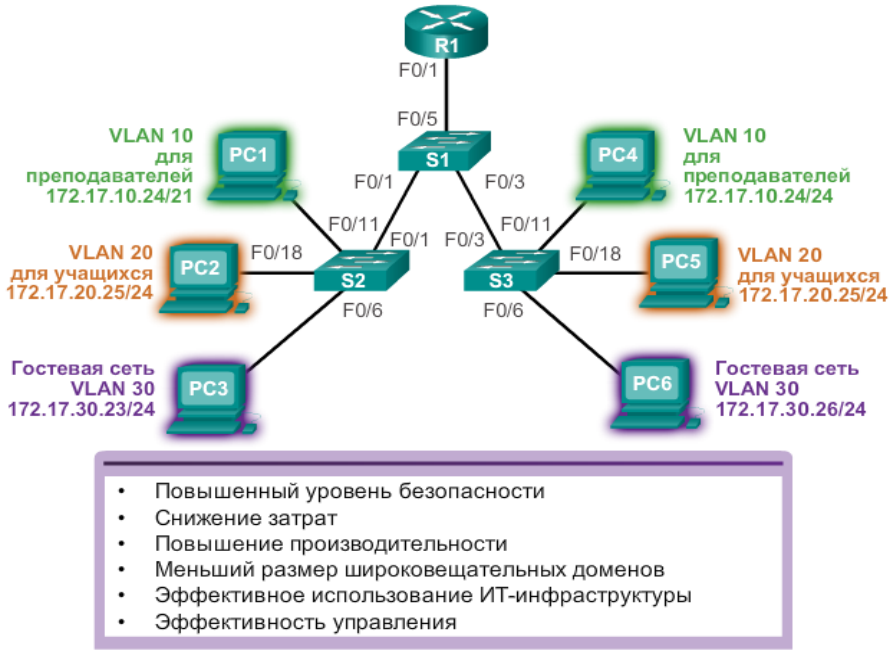

Рисунок 1.4 – Преимущества виртуальных локальных сетей

Типы виртуальных локальных сетей.

В современных сетях используется множество различных типов сетей VLAN. Некоторые типы VLAN определяются классами трафика. Другие типы VLAN обусловлены функциями, которые они выполняют.

Виртуальная локальная сеть для данных.

Виртуальная локальная сеть для данных — это сеть VLAN, которая настроена специально для передачи трафика, генерируемого пользователем. Сеть VLAN, передающая голосовой трафик или трафик управления, не является сетью VLAN для передачи данных. Рекомендуется отделять голосовой и управляющий трафик от трафика данных. VLAN для передачи данных иногда называют пользовательской сетью VLAN. Сети VLAN для данных используются для разделения сети на группы пользователей или устройств.

Сеть VLAN по умолчанию.

Все порты коммутатора становятся частью VLAN по умолчанию после первоначальной загрузки коммутатора. Порты коммутатора, находящиеся в сети VLAN по умолчанию, являются частью одного широковещательного домена. Благодаря этому любое устройство, подключённое к любому порту коммутатора, может обмениваться данными с другими устройствами на других портах коммутатора. Сетью VLAN по умолчанию для коммутаторов Cisco установлена VLAN 1. На рисунке команда *show vlan brief* была выполнена на коммутаторе, настроенном по умолчанию. Обратите внимание, что на все порты по умолчанию назначены сети VLAN 1.

VLAN 1 поддерживает все функции любой сети VLAN, однако её нельзя переименовать или удалить. По умолчанию весь управляющий трафик 2-го уровня связан с сетью VLAN 1.

Native VLAN.

Сеть native VLAN назначена транковому порту 802.1Q. Транковые порты — это каналы между коммутаторами, которые поддерживают передачу трафика, связанного с более чем одной сетью VLAN. Транковый порт 802.1Q поддерживает трафик, поступающий от нескольких VLAN (тегированный трафик), а также трафик, который поступает не от VLAN (нетегированный трафик). Тегированным называется трафик, для которого в исходный заголовок кадра Ethernet вставлен 4-байтовый тег, определяющий сеть VLAN, к которой относится этот кадр. Транковый порт 802.1Q размещает нетегированный трафик в сети native VLAN, которой по умолчанию является VLAN 1.

Сети native VLAN определены в спецификации IEEE 802.1Q для обеспечения обратной совместимости с нетегированным трафиком, характерным для устаревших сценариев локальных сетей. Сеть native VLAN служит общим идентификатором на противоположных концах транкового канала.

Рекомендуется настроить native VLAN как неиспользуемую VLAN, отличающуюся от сети VLAN 1 и других VLAN. Фактически принято выделять фиксированную VLAN для выполнения роли сети native VLAN для всех транковых портов в коммутируемом домене.

Управляющая VLAN.

Управляющая VLAN — это любая сеть VLAN, настроенная для доступа к функциям управления коммутатора. Сеть VLAN 1 по умолчанию является управляющей VLAN. Для создания управляющей VLAN интерфейсу SVI коммутатора данной VLAN назначаются IP-адрес и маска подсети, благодаря чему коммутатором можно управлять через протоколы HTTP, Telnet, SSH или SNMP. Поскольку в исходной настройке коммутатора Cisco VLAN 1 является сетью VLAN по умолчанию, VLAN 1 не следует использовать в качестве управляющей VLAN.

В прошлом управляющая VLAN для коммутатора 2960 была единственным активным интерфейсом SVI. В версиях ОС Cisco IOS 15.x для коммутаторов Catalyst серии 2960 возможна поддержка более одного активного интерфейса SVI. В версиях ОС Cisco IOS 15.x необходимо документировать определённый активный интерфейс SVI, назначенный для удалённого управления. Несмотря на то что теоретически коммутатор может обладать более чем одной управляющей VLAN, использование нескольких сетей данного типа увеличивает подверженность сетевым атакам.

На рисунке 1.5 все порты назначены сети VLAN 1 по умолчанию. Ни одна native VLAN не назначена явно, и ни одна другая сеть VLAN не является активной. Таким образом, сети native VLAN и управляющая VLAN совпадают. Подобная настройка считается угрозой безопасности.

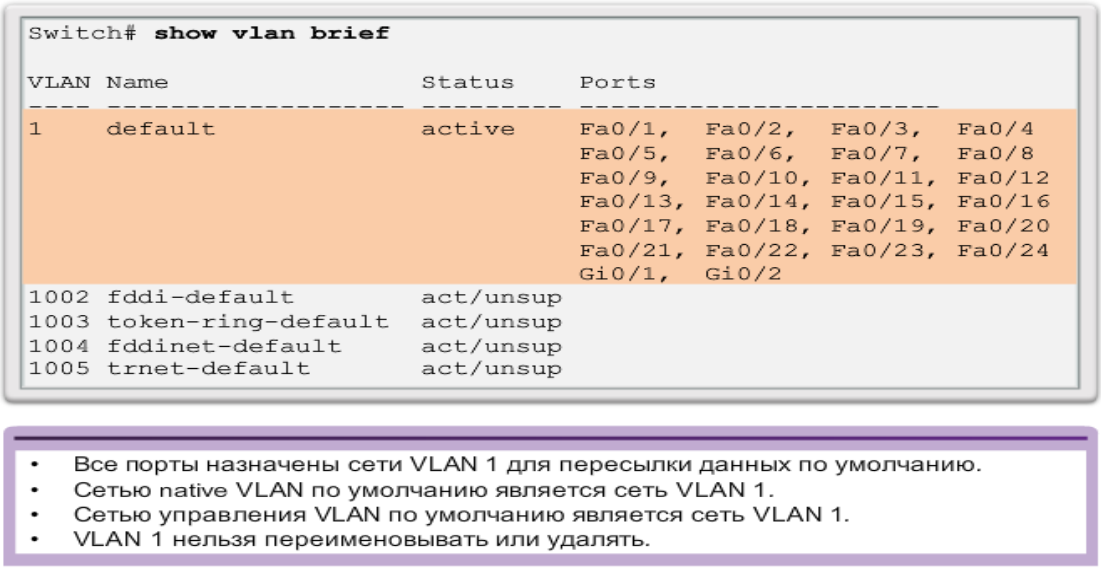

Рисунок 1.5 – VLAN 1

Голосовые сети VLAN.

Для поддержки передачи голоса по IP (VoIP) требуется отдельная сеть VLAN. Для VoIP-трафика требуется:

- гарантированная полоса пропускания для обеспечения высокого качества голосовой передачи;
- приоритет передачи перед другими типами сетевого трафика;
- возможность маршрутизации в обход перегруженных участков;
- задержка менее 150 мс по всей сети.

Для того чтобы соответствовать этим требованиям, вся сеть должна быть специально спроектирована для поддержки VoIP. В рамках данного курса не рассматриваются особенности настройки сети для поддержки VoIP, однако краткая информация о том, как голосовая VLAN работает между коммутатором, IP-телефоном Cisco и компьютером, будет полезна.

На рисунке 1.6 VLAN 150 предназначена для передачи голосового трафика. Компьютер учащегося PC5 подключён к IP-телефону Cisco, а телефон подключён к коммутатору S3. PC5 находится в сети VLAN 20, которая используется для передачи данных учащихся.

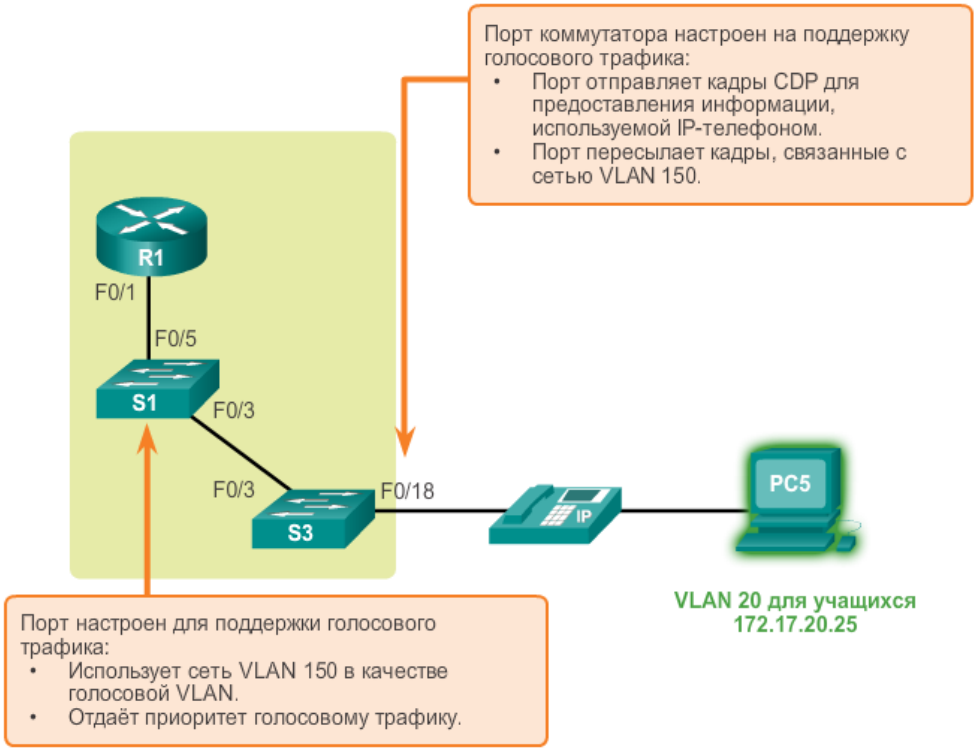

Рисунок 1.6 – Голосовая сеть VLAN

2.1 Протокол виртуального магистрального канала

Транк — это канал типа «точка-точка» между двумя сетевыми устройствами, который поддерживает более одной сети VLAN. Транк виртуальных сетей расширяет сети VLAN по всей сети. Cisco поддерживает стандарт IEEE 802.1Q для координации транков в интерфейсах Fast Ethernet, Gigabit Ethernet и 10-Gigabit Ethernet.

Использование сетей VLAN без транковых каналов существенно снижает полезные возможности VLAN. Транки виртуальных сетей обеспечивают распространение всего трафика VLAN между коммутаторами так, чтобы устройства, находящиеся в одной сети VLAN, но подключённые к разным коммутаторам, могли обмениваться данными без вмешательства маршрутизатора.

Транк виртуальных сетей не принадлежит какой-либо определённой сети VLAN, а, скорее, является «кабельным каналом» передачи многих VLAN между коммутаторами и маршрутизаторами. Транк может также использоваться между сетевым устройством и сервером или другим устройством, оснащённым соответствующим сетевым адаптером с поддержкой 802.1Q. Пример транковых линий между VLAN приведен на рисунке 1.7.

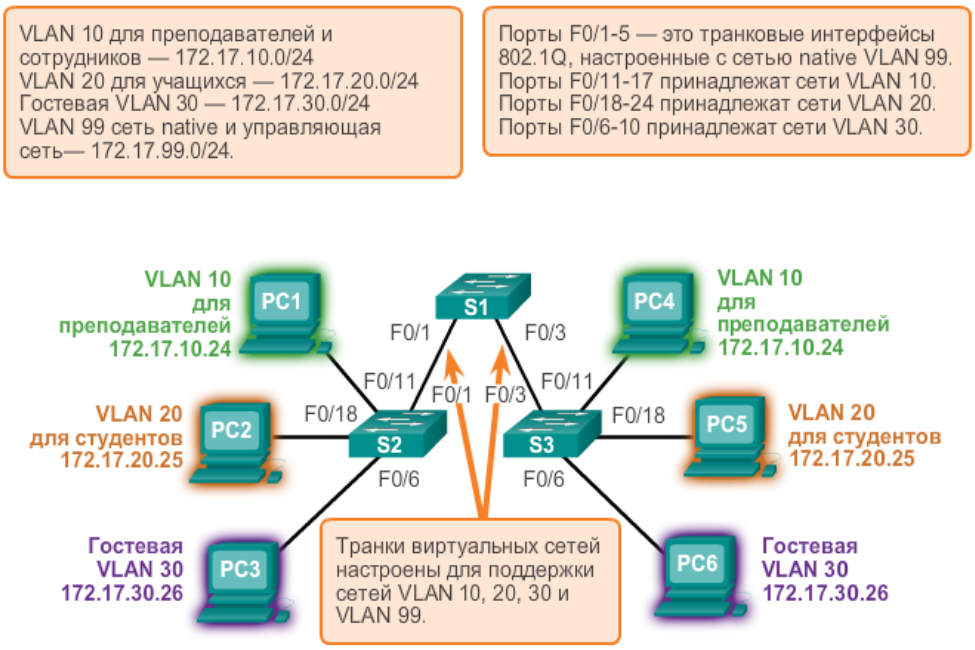

Рисунок 1.7 – Транки виртуальных сетей

2.2.1 Сети native VLAN и тегирование стандарта 802.1Q. Тегированные кадры в сети native VLAN.

Некоторые устройства, поддерживающие транковую связь, добавляют метку в трафик сети native VLAN. Управляющий трафик, отправляемый в сети native VLAN, тегировать не следует. Если транковый порт 802.1Q получает тегированный кадр с таким же идентификатором VLAN, как у сети native VLAN, то он отбрасывает кадр. Следовательно, при настройке порта коммутатора в коммутаторе Cisco настраивайте устройства таким образом, чтобы они не отправляли тегированные кадры по сети native VLAN. К устройствам от других производителей, которые поддерживают тегированные кадры в сети native VLAN, относятся IP-телефоны, серверы, маршрутизаторы и коммутаторы не от Cisco.

Нетегированные кадры в сети native VLAN.

Когда транковый порт коммутатора Cisco получает нетегированные кадры (которые редко встречаются в хорошо спроектированной сети), он пересылает эти кадры в сеть native VLAN. Если с сетью native VLAN не связаны никакие устройства (что бывает довольно часто), а также нет других транковых портов (что также часто случается), то кадр отбрасывается. Сетью native VLAN по умолчанию является сеть VLAN 1. При настройке транкового порта 802.1Q порту идентификатора VLAN по умолчанию (PVID) присваивают значение идентификатора сети native VLAN. Весь нетегированный трафик, поступающий в порт 802.1Q или из него, пересылается в соответствии со значением PVID. Например, если сеть VLAN 99 настроена в качестве native VLAN, то значение PVID равно 99, а весь нетегированный трафик пересылается в сеть VLAN 99.

Если сеть native VLAN не была перенастроена, то значение PVID присваивается равным 1.

На рисунке 1.8 компьютер PC1 подключен к транковому каналу 802.1Q с помощью концентратора. PC1 отправляет нетегированный трафик, который коммутаторы связывают с сетью native VLAN, настроенной на транковых портах, и пересылают его соответствующим образом. Тегированный трафик в транковом канале, полученный компьютером PC1, отбрасывается. В этом сценарии сеть является плохо спроектированной по нескольким причинам: в ней используется концентратор, имеется узел, подключённый к транковому каналу, и это означает, что существуют порты доступа коммутаторов, назначенные сети native VLAN. Но в этом сценарии иллюстрируется необходимость в спецификации IEEE 802.1Q для native VLAN как средства обработки устаревших сценариев.

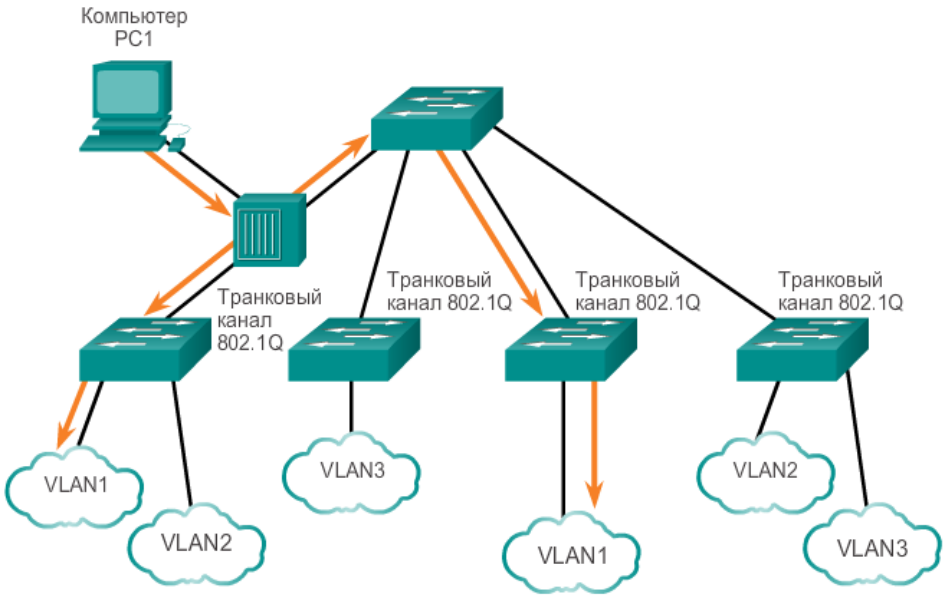

Рисунок 1.8 – Сети native VLAN на транковом канале 802.1Q

2.2.2 Тегирование голосовой VLAN.

Не забывайте, что для поддержки VoIP требуется отдельная голосовая VLAN.

Порт доступа, используемый для подключения IP-телефона Cisco, может быть настроен для использования двух отдельных сетей VLAN: одна сеть VLAN для голосового трафика, а другая сеть VLAN для трафика данных от устройства, подключенного к телефону. Канал между коммутатором и IP-телефоном служит транковым каналом для передачи и голосового трафика, и трафика данных.

IP-телефон Cisco содержит встроенный коммутатор 10/100 на 3 порта. Порты обеспечивают выделенные подключения следующим устройствам:

- порт 1 подключается к коммутатору или другому устройству VoIP;
- порт 2 является внутренним интерфейсом 10/100, через который передаётся трафик IP-телефона;
- порт 3 (порт доступа) подключается к ПК или другому устройству.

На коммутаторе доступ настроен для отправки пакетов протокола CDP, указывающих подключённому IP-телефону отправлять голосовой трафик на коммутатор одним из трёх способов, в зависимости от типа трафика:

- в голосовой VLAN, тегированной значением приоритета класса обслуживания (CoS) уровня 2;
- в VLAN доступа, тегированной значением приоритета CoS уровня 2;
- в нетегированной VLAN доступа (без значения приоритета CoS уровня 2).

На рисунке 2.9 компьютер учащегося PC5 подключён к IP-телефону Cisco, а телефон подключён к коммутатору S3. VLAN 150 предназначена для передачи голосового трафика, а PC5 находится в VLAN 20, используемой для данных учащихся.

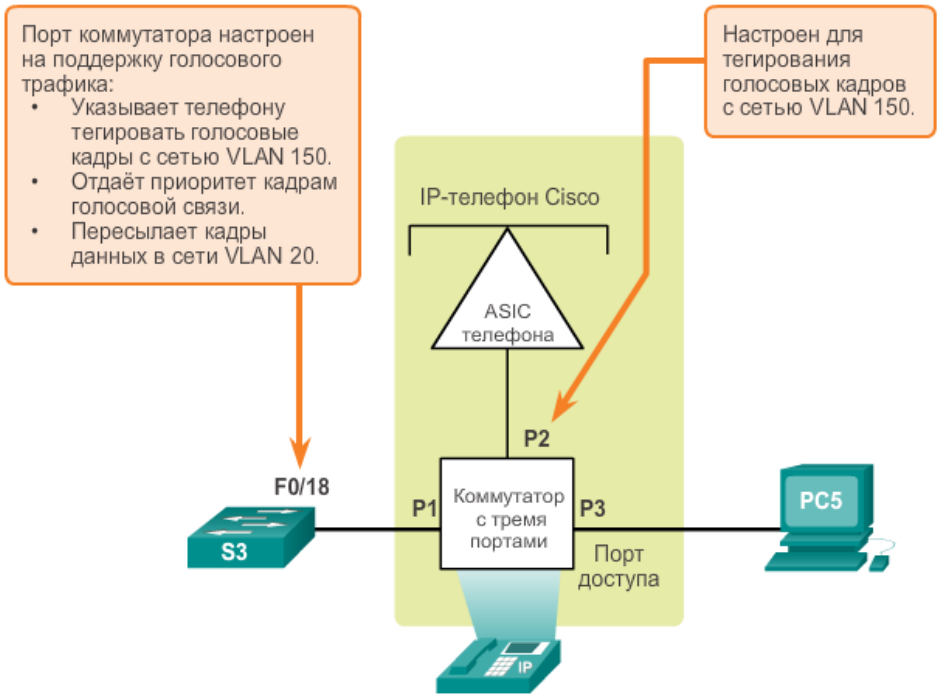

Рисунок 1.9 – Тегирование голосовой VLAN

1.2 Оборудование комплекса лабораторных работ

В комплексе лабораторных работ применено оборудование компании Cisco Systems – являющейся безусловным лидером в классе оборудования для полстроения надежных, высокопроизводительных и защищенных компьютерных сетей.

Использованы коммутаторы 2960 и маршрутизаторы 2811. К тому же это оборудование наиболее доступно Алматинскому Университету Энергетики и Связи (в данный момент находятся в наличии кафедры КТ).

Коммутаторы – Cisco Catalyst 2960

Рисунок 1.10 – Внешний вид коммутаторов семейства Cisco Catalyst 2960

Интеллектуальные Ethernet-коммутаторы Cisco Catalyst серии 2960 (Cisco Catalyst 2960 Series Intelligent Ethernet Switch) позволяют реализовать расширенные сервисы в локальных сетях крупных и средних предприятий, а также в сетях филиалов. Представители этого семейства автономных коммутаторов с фиксированной конфигурацией обеспечивают подключение рабочих мест на скоростях 10/100 Fast Ethernet и 10/100/1000 Gigabit Ethernet.

Возможности моделей серии:

- подключение: подключения Fast Ethernet и Gigabit Ethernet в конфигурациях с 8, 24 и 48 портами;
- питание устройств по витой паре: конфигурации с 24 портами с полной поддержкой PoE и 24 портами (с поддержкой PoE на 8 портах);
- интегрированные функции безопасности, включая контроль доступа в сеть (NAC);
- расширенные возможности управления качеством обслуживания (QoS) и обеспечения отказоустойчивости;
- интеллектуальные сервисы на границе сети;
- упрощение сетевого управления.

Предлагаемое для коммутаторов Catalyst серии 2960 программное обеспечение Cisco Network Assistant обеспечивает централизованное управление коммутаторами, маршрутизаторами и беспроводными точками доступа Cisco. Поставляемое бесплатно, это приложение включает в себя простые в использовании мастера настройки, которые значительно облегчают реализацию конвергентных сетей и интеллектуальных сетевых сервисов.

Рисунок 1.11 – внешний вид маршрутизатора Cisco 2811

Архитектура маршрутизаторов с интегрированными услугами семейства Cisco 2800 базируется на архитектуре мощных мультисервисных маршрутизаторов доступа серии Cisco 2600, предлагая дополнительно встроенные функции безопасности, существенно улучшенную производительность и расширенный объем памяти, а также новые интерфейсы высокой плотности. Благодаря достигнутым показателям производительности, доступности и надежности маршрутизаторы серии Cisco 2800 оказываются незаменимыми для критически важных бизнес-приложений, используемых в наиболее сложных рабочих условиях.

Показатели производительности и плотности портов маршрутизаторов с интегрированными услугами серии Cisco 2800 отвечают требованиям, предъявляемым предприятиями среднего размера, а также малыми и средними филиалами крупных предприятий к защищенным, одновременно предоставляемым услугам, а также требованиям к управляемым услугам, предъявляемым операторами связи – без ущерба для производительности маршрутизатора.

Работая под управлением программного обеспечения Cisco IOS, маршрутизаторы серии Cisco 2800 поддерживают концепцию сети с возможностями самозащиты Cisco Self-Defending Network – благодаря улучшенным функциям безопасности и возможностям управления, таким как аппаратная акселерация шифрования, поддержка IPSec VPN (с использованием алгоритмов шифрования AES, 3DES, DES), межсетевой экран, система предотвращения вторжений (IPS), контроль за доступом к сети (NAC) и фильтрация по URL. Предустановленная на всех маршрутизаторах серии Cisco 2800, интуитивно-понятная система управления с Web-интерфейсом Cisco Router and Security Device Manager (SDM) существенно упрощает управление и конфигурирование маршрутизатора.

Маршрутизаторы серии Cisco 2800 поддерживают самые эффективные в отрасли решения IP-коммуникаций. Начиная от обычной телефонии и заканчивая такими функциями, как обработка мультимедийных вызовов, система передачи сообщений, автоматическая операторская служба – все это

предоставляет пользователям достаточно широкие возможности по адаптации решений под свои конкретные требования. Маршрутизаторы серии Cisco 2800 являются идеальным решением для тех, кто желает сократить организационные расходы и сложность сети за счет конвергенции сети голосовой связи и сети передачи данных.

Модульный маршрутизатор с интеграцией сервисов (Integrated Services Routers, ISR), оптимизированный для безопасной передачи данных, голоса и видео на скорости канала связи.

По сравнению с предидущей серией маршрутизаторов (2600) обеспечивает значительный прирост производительности, новые интегрированные сервисы и значительно увеличенную плотность интерфейсов при сохранении обратной совместимости с более чем 90 существующими на сегодня модулями.

Маршрутизатор Cisco 2811, как и вся серия модульных маршрутизаторов 2800 отличается гибкой модульной конструкцией. Доступны слоты NME, для установки сетевых модулей, слоты HWIC для установки интерфейсных модулей, Слоты EVM для поддержки дополнительных голосовых интерфейсов, а также слоты PVDM и гнезда AIM на системной плате маршрутизатора для установки модулей обработки голоса и сервисных модулей соответственно. Слоты NME и HWIC имеют обратную совместимость с модулями NM и WIC соответственно.

Все маршрутизаторы серии 2800 имеют интегрированнные средства аппаратного ускорения шифрования, обеспечивают функциональность системы обнаружения вторжений и межсетевого экрана.

Ключевые особенности:

- высокая производительность;
- модульная архитектура;
- аппаратная поддержка средств обеспечения безопасности;
- возможность использования технологии передачи электроэнергии по сетям Ethernet (PoE).

На основе проведенного анализа существующей методики обучения по безопасности компьютерных систем и сетей в АУЭС (кафедра КТ) 2014-2015 годах была разработана данная методика, которая позволяет получить наиболее полные знания и твердые навыки по основным аспектам построения систем, обеспечения защиты информации в корпоративных сетях. Данная методика знакомит слушателя с основными возможностями используемого оборудования.

Комплекс лабораторных работ по типу используемого оборудования (Cisco) не имеет аналогов в АУЭС.

ГЛАВА 2 КОМПЬЮТЕРНЫЕ СЕТИ

2.1 Использование сетей в повседневной жизни

Среди всех основных потребностей человеческого существования необходимость взаимодействовать с другими людьми является одной из самых важных потребностей человека. Общение почти так же важно для нас, как воздух, вода, пища и кров.

Способы общения постоянно меняются и развиваются. Когда-то мы были ограничены индивидуальным общением, но прорыв в сфере технологий значительно расширил границы коммуникации. От наскальных рисунков к печатному станку, радио и телевидению — каждая новая разработка улучшала и расширяла нашу способность связываться и общаться с другими людьми.

Создание и объединение надёжных сетей передачи данных оказало глубокое влияние на связь и стало новой платформой, на которой происходят современные коммуникации.

В современном мире за счёт использования сетей мы связаны друг с другом как никогда раньше. Люди с творческими идеями могут немедленно связаться с другими нужными людьми, чтобы воплотить свои идеи в реальность. Новости и открытия становятся известными во всем мире в считанные секунды. Люди могут играть в игры с друзьями, которые находятся на других континентах.

Сети объединяют людей и способствуют спонтанному общению. Каждый может подключиться, поделиться информацией и внести свой вклад.

2.2 Использование сетей помогает в обучении

Сети и Интернет изменили все, что мы делаем: то, как мы учимся, общаемся, работаем и развлекаемся.

Изменение способов обучения

Коммуникация, совместная работа и вовлечённость — три основных конструктивных элемента образования. Образовательные учреждения постоянно стремятся усовершенствовать эти процессы для стимулирования распространения знаний. Традиционные способы обучения обеспечивают главным образом два источника опыта, из которых студенты могут получить сведения: учебник и преподаватель. Эти два источника ограничены как в формате, так и во времени предоставления информации.

Сети изменили способ, с помощью которого мы учимся. Надёжные и устойчиво работающие сети поддерживают и улучшают среду для обучения. С их помощью можно предоставлять учебные материалы в самых разных форматах, включая интерактивные занятия, контрольные работы и обратную связь. Как показано на рисунке 2.1, сети:

поддерживают создание виртуальных классов;

обеспечивают видеосвязь по запросу;

создают пространства для совместной работы учащихся;

делают возможным мобильное обучение.

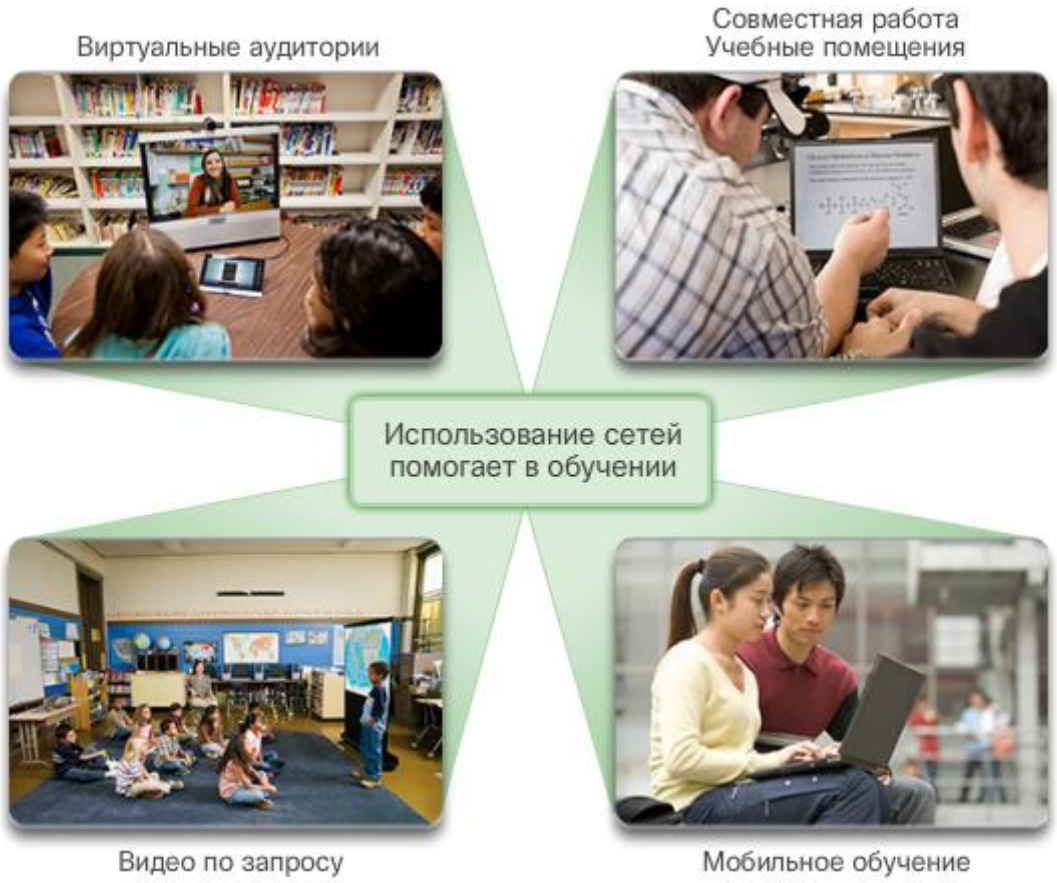

Рисунок 2.1 – Использование сетей помогает в обучении

Получить образование у высококвалифицированного преподавателя теперь возможно не только для студентов проживающих в непосредственной близости от места, где работает данный преподаватель. Дистанционное онлайн-обучение преодолело географические барьеры, увеличив возможности учащихся. Интерактивные курсы (электронное обучение) теперь можно получать по сети. Эти курсы могут содержать данные (текст, ссылки), голос и видео, доступные учащимся в любое время и из любого места. Группы для обсуждения и доски сообщений позволяют учащимся совместно работать с преподавателем, с другими учащимися в классе или с учащимися по всему

миру. Можно объединить занятия под руководством преподавателя и интерактивные учебные программы в смешанные курсы, чтобы получить максимальную пользу от двух способов обучения. Рис. 2 — видеоролик об изменениях, произошедших в учебных классах.

Помимо предоставления преимуществ учащимся сети усовершенствовали управление и администрирование образования. Некоторые из этих функций в режиме онлайн включают в себя регистрацию учащегося, выставление оценок и отслеживание совершенствования знаний.

2.3 Сети различных масштабов

Существуют сети любого размера, от простых сетей, состоящих из двух компьютеров, до систем, соединяющих миллионы устройств.

В небольших сетях, сетях домашнего офиса возможно организовать общий доступ к ресурсам, таким как принтеры, документы, изображения, музыка между локальными компьютерами.

Сети малых и домашних офисов часто настраиваются людьми, которые работают из дома или удалённого офиса и которым необходимо подключение к корпоративной сети или другим централизованным ресурсам. Кроме того, индивидуальные предприниматели используют сети малого и домашнего офиса в рекламных целях и для продажи продукции, заказа расходных материалов и взаимодействия с клиентами. Как правило, сетевая связь эффективнее и дешевле традиционных методов связи, например, почты или междугородных телефонных звонков.

На предприятиях и в крупных организациях сети могут использоваться в еще более обширном масштабе, чтобы позволить сотрудникам собирать, хранить и получать информацию на сетевых серверах. Кроме того, сети позволяют наладить быструю связь в виде электронной почты, обмена мгновенными сообщениями, а также функций совместной работы между сотрудниками. В дополнение к внутренним организационным преимуществам большинство компаний применяет сети для предоставления продуктов и услуг заказчикам через подключение к Интернету.

Интернет — это крупнейшая сеть во всем мире. На самом деле понятие «Интернет» означает «сеть всех сетей». Интернет буквально представляет собой объединение подключённых друг к другу частных и общедоступных сетей (некоторые из них были описаны выше). Корпоративные сети, сети малого

бизнеса и даже домашние сети обычно обеспечивают общий доступ к Интернету.

Это невероятно, насколько быстро Интернет стал неотъемлемой частью нашей повседневной жизни.

Рисунок 2.2 – Сети различных масштабов

2.4 Компоненты сети

Маршрут, по которому сообщение идет от источника к месту назначения, может быть простым, например один кабель, соединяющий один компьютер с другим, или сложным, как сеть, буквально охватывающая весь мир. Инфраструктура сети — это платформа, поддерживающая конкретную сеть. Она выполняет роль стабильного и надежного канала для передачи данных.

Инфраструктура сети включает в себя три категории компонентов сети:

Устройства

Среда

Сервисы

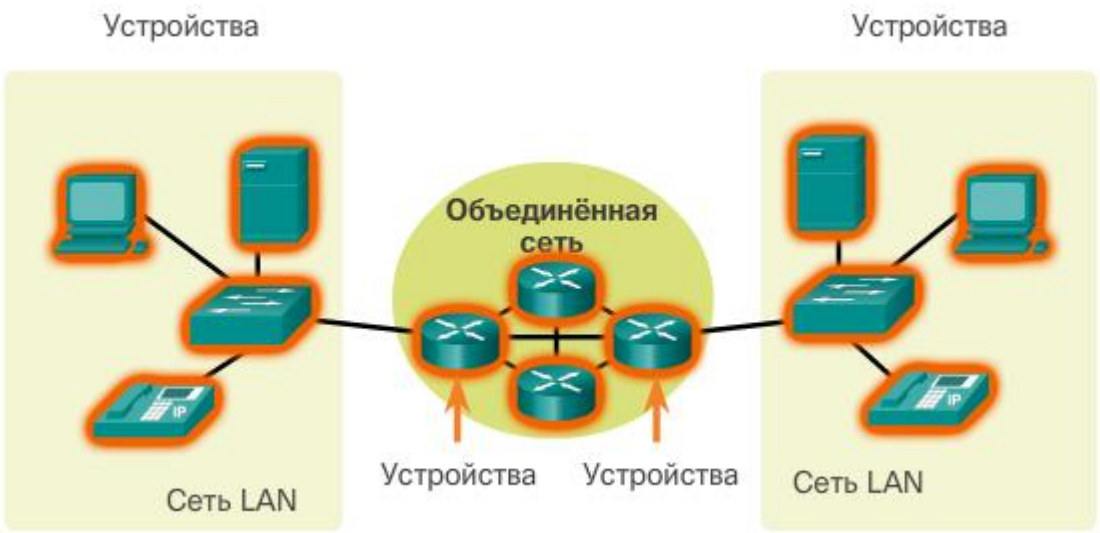

Рисунок 2.3 – Устройства сети

Устройства и среда — это физические элементы или оборудование сети. Оборудование часто является видимой частью сетевой платформы — ноутбук, ПК, коммутатор, маршрутизатор, точка беспроводного доступа или кабели, используемые для соединения устройств. Некоторые компоненты являются невидимыми. В случае беспроводных сетей сообщения передаются с помощью незримого радиочастотного или инфракрасного излучения.

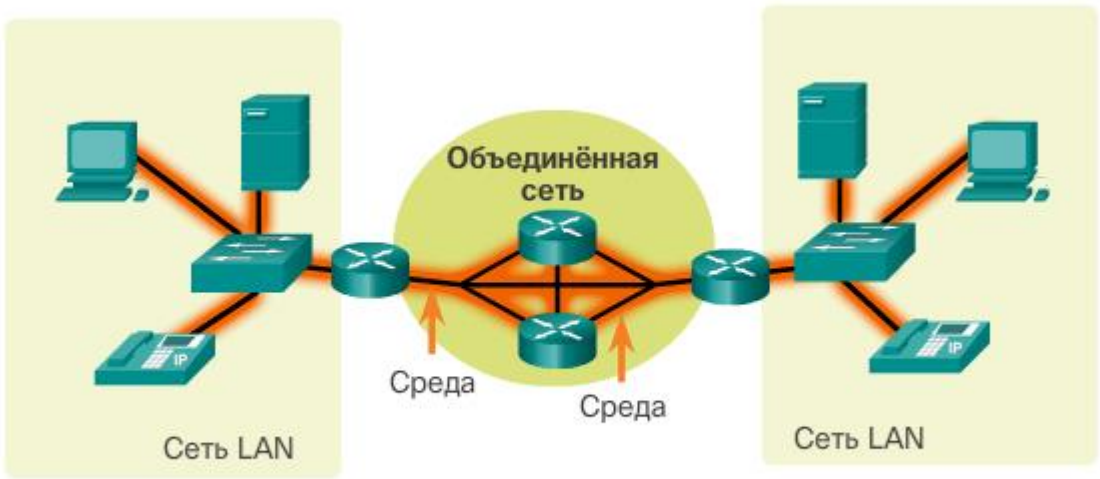

Рисунок 2.4 – Среда передачи информации

Компоненты сети используются для предоставления сервисов и процессов. Это коммуникационные программы, называемые программным обеспечением, которые работают на сетевых устройствах. Сетевой сервис предоставляет данные в ответ на запрос. Сервисы включают в себя множество

сетевых приложений, которые люди используют ежедневно, например, сервисы электронной почты и сервисы веб-хостинга для веб-сайтов. Процессы обеспечивают функциональность, которая направляет и перемещает сообщения в сети. Процессы менее очевидны для нас, но критически важны для работы сетей.

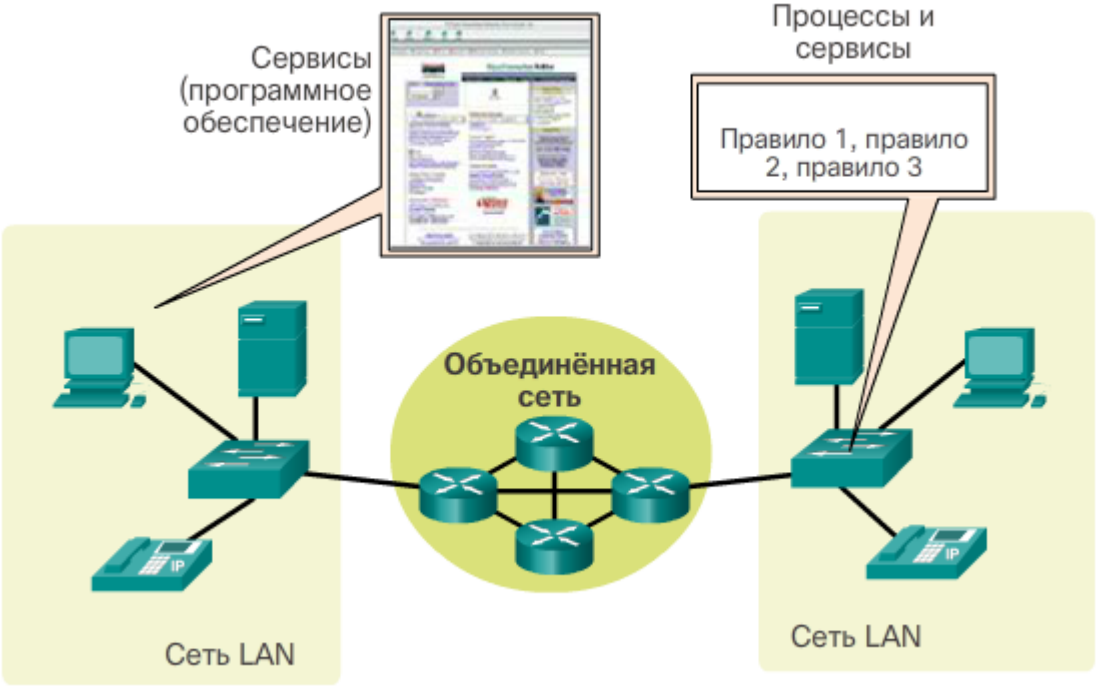

Рисунок 2.5 – Сервисы компьютерной сети

2.5 Схемы топологий

Схемы топологий необходимы для каждого, кто работает с сетью. Они обеспечивают визуальную карту соединений в сети.

Существует два типа схем топологии:

Схемы физической топологии — физическое расположение промежуточных устройств, настроенных портов и прокладки кабеля.

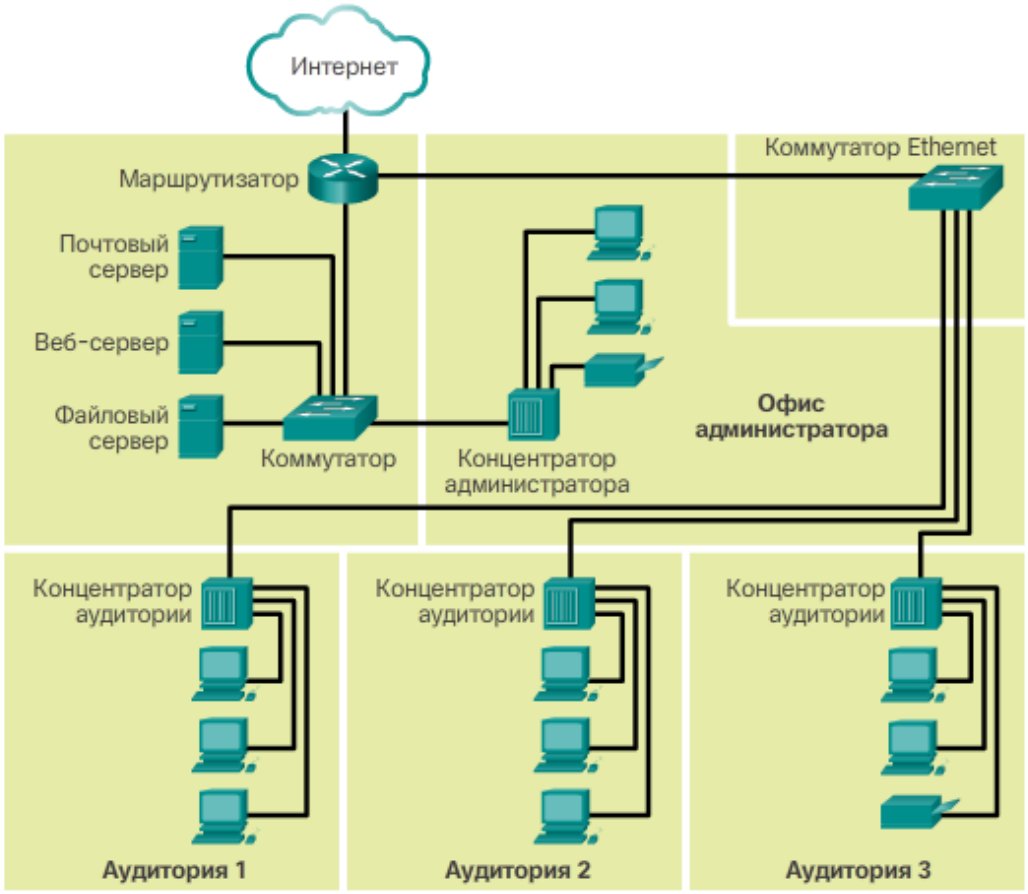

Рисунок 2.6 – Физическая топология сети

Схемы логической топологии — определение устройств, портов и схемы IP-адресации.

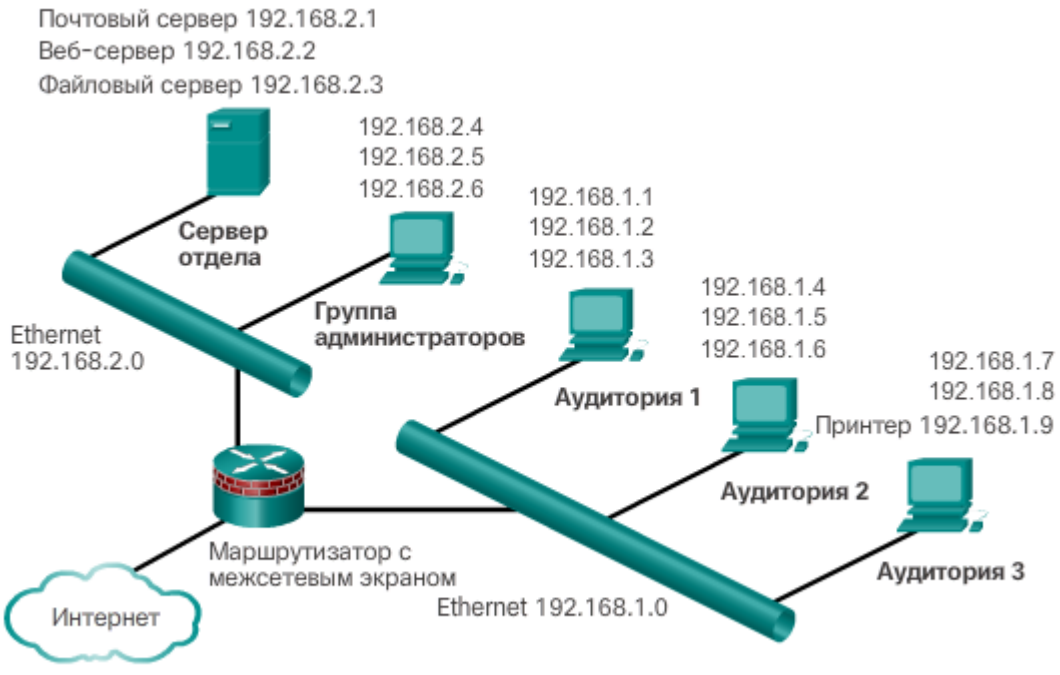

Рисунок 2.7 – Логическая топология сети

2.6 Типы сетей

Сетевые инфраструктуры могут в значительной мере отличаться по следующим критериям:

Размер обслуживаемой территории

Количество подключённых пользователей

Число и типы доступных сервисов

На рисунке ниже представлены два наиболее распространённых типа сетевой инфраструктуры:

Локальная сеть (LAN) — сетевая инфраструктура, которая обеспечивает доступ пользователям и оконечным устройствам в небольшой географической области.

Глобальная сеть (WAN) — сетевая инфраструктура, которая предоставляет доступ к другим сетям на обширной географической области.

К другим типам сетей относятся:

Муниципальная сеть (MAN) — сетевая инфраструктура, которая охватывает физическую область больше, чем LAN, но меньше глобальной сети (WAN) (например, город). Как правило, управление MAN осуществляется одной организацией, например, крупным предприятием.

Беспроводная локальная сеть (LAN) Беспроводные локальные сети (WLAN) аналогичны сетям LAN, но соединяют пользователей и оконечные устройства небольшой географической области с помощью беспроводной связи.

Сеть хранения данных (SAN) — сетевая инфраструктура, разработанная для поддержки файловых серверов и обеспечения хранения данных, их получения из хранилища и репликации. Она включает в себя высокопроизводительные серверы, дисковые массивы и технологию соединений Fibre Channel.

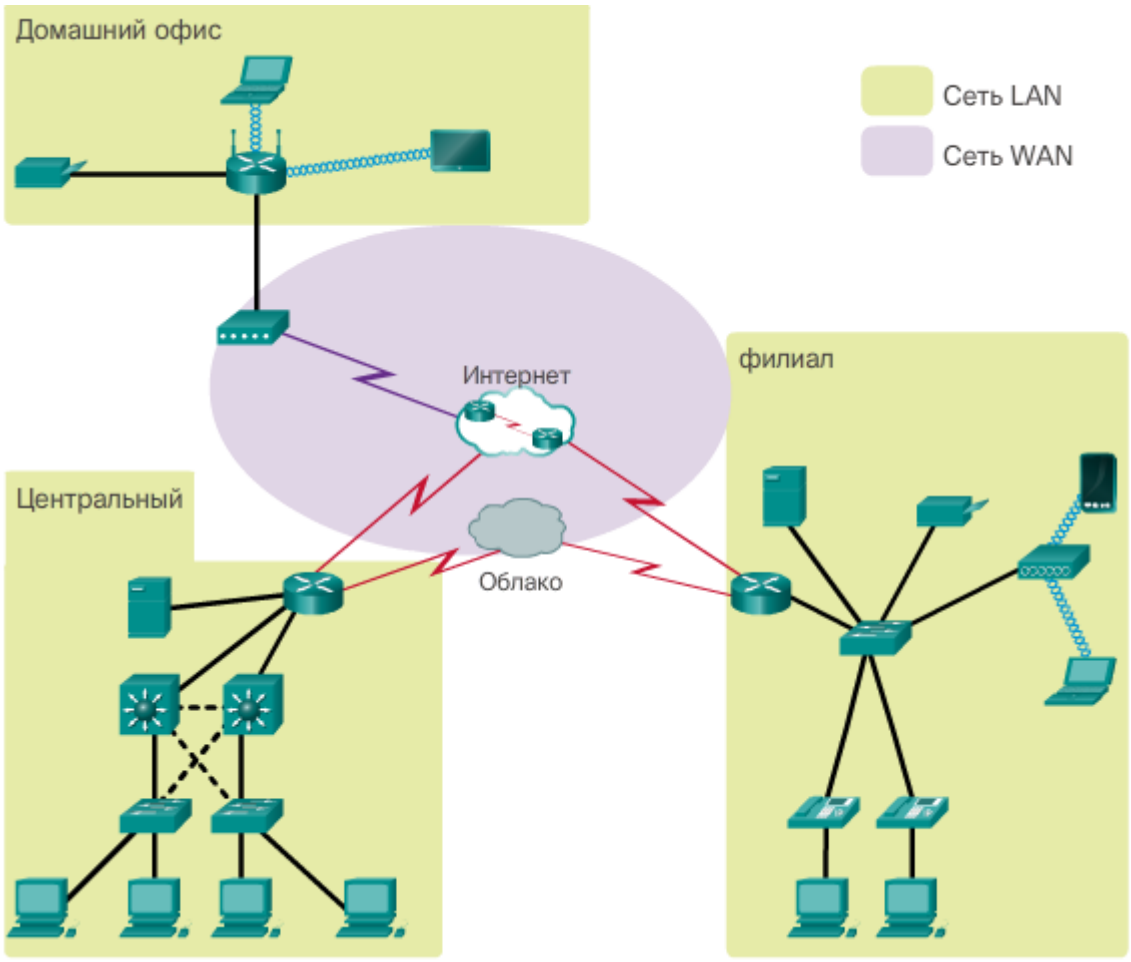

Рисунок 2.8 – Типы сетей (Локальная сеть и Глобальная сеть)

2.6.1 Системы локальных сетей

Локальные сети (LAN) — сетевая инфраструктура, которая охватывает небольшую географическую область. Основные компоненты LAN:

Локальные сети связывают оконечные устройства в ограниченной области, например, в доме, школе, офисном здании или комплексе зданий.

Локальная сеть обычно администрируется одной организацией или частным лицом. Администратор управляет политикой безопасности и контролем доступа на сетевом уровне.

Локальные сети предоставляют высокоскоростной доступ к внутренним оконечным и промежуточным устройствам.

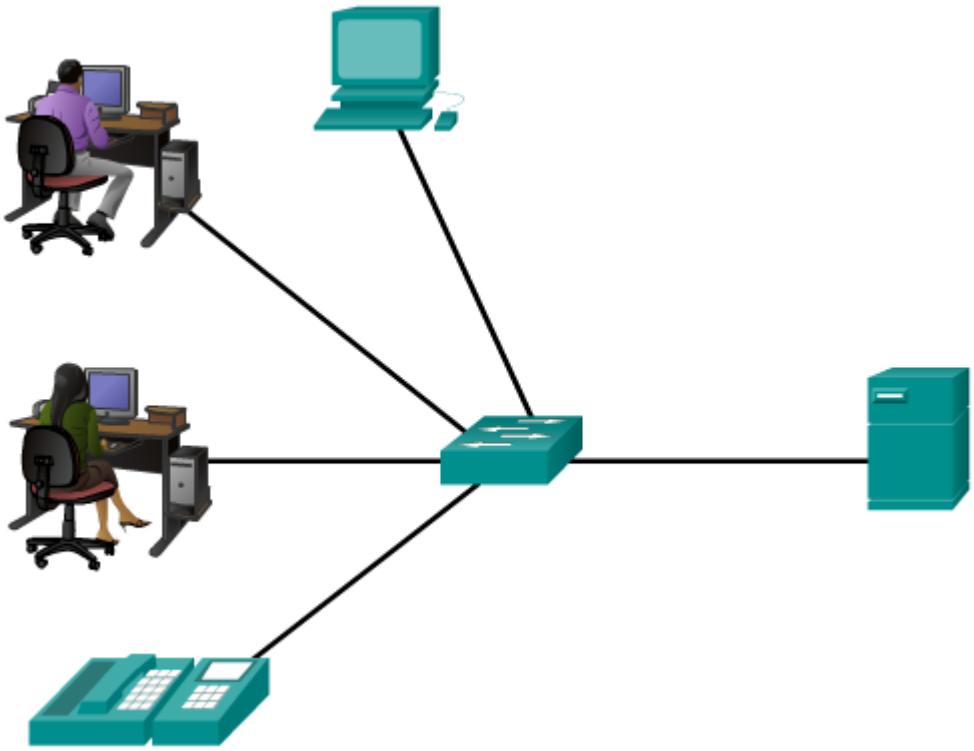

Рисунок 2.9 – Локальная сеть

2.6.2 Глобальные сети

Глобальные сети (WAN) — сетевая инфраструктура, которая охватывает обширную географическую область. Управление глобальными сетями обычно осуществляется операторами связи (SP) или Интернет-провайдерами (ISP).

Основные компоненты WAN

WAN связывают локальные сети в обширных географических областях, таких как города, регионы, страны или континенты.

Управление глобальными сетями обычно осуществляется различными операторами связи.

Глобальные сети обычно обеспечивают более низкоскоростные соединения между локальными сетями.

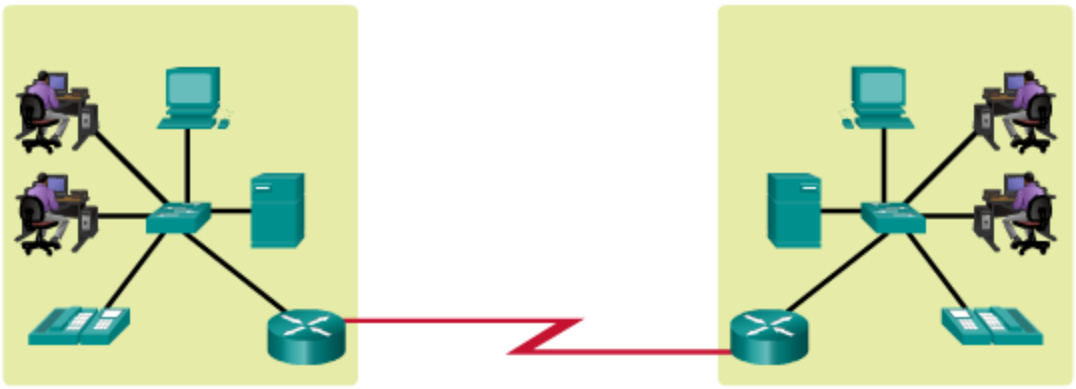

Рисунок 2.10 – Глобальная сеть

2.6.3 Интернет

Хотя есть преимущества в использовании LAN или WAN, большинству людей необходима связь с ресурсом в другой сети, за пределами локальной сети в рамках дома, сети учебного заведения или организации. Для этого используется Интернет.

Как показано на рисунке, Интернет — это общемировой конгломерат взаимосвязанных сетей, взаимодействующих друг с другом для обмена информацией на основе общих стандартов. Пользователи, подключившиеся к Интернету по телефонной линии, оптоволоконному кабелю, беспроводной связи или через спутник, могут обмениваться данными в самых разнообразных формах.

Интернет представляет собой конгломерат сетей, который не принадлежит какому-либо человеку или группе. Обеспечение эффективного общения с помощью данной разнообразной инфраструктуры требует применения последовательных и общепризнанных технологий и стандартов, а также совместной работы многих учреждений, администрирующих сети. Существуют организации, созданные для поддержания структуры и стандартизации протоколов и процессов Интернета. Эти организации включают в себя Инженерную группу по развитию Интернета (IETF), Интернет-корпорацию по присвоенным именам и номерам (ICANN) и Совет по архитектуре Интернета (IAB), а также многие другие.

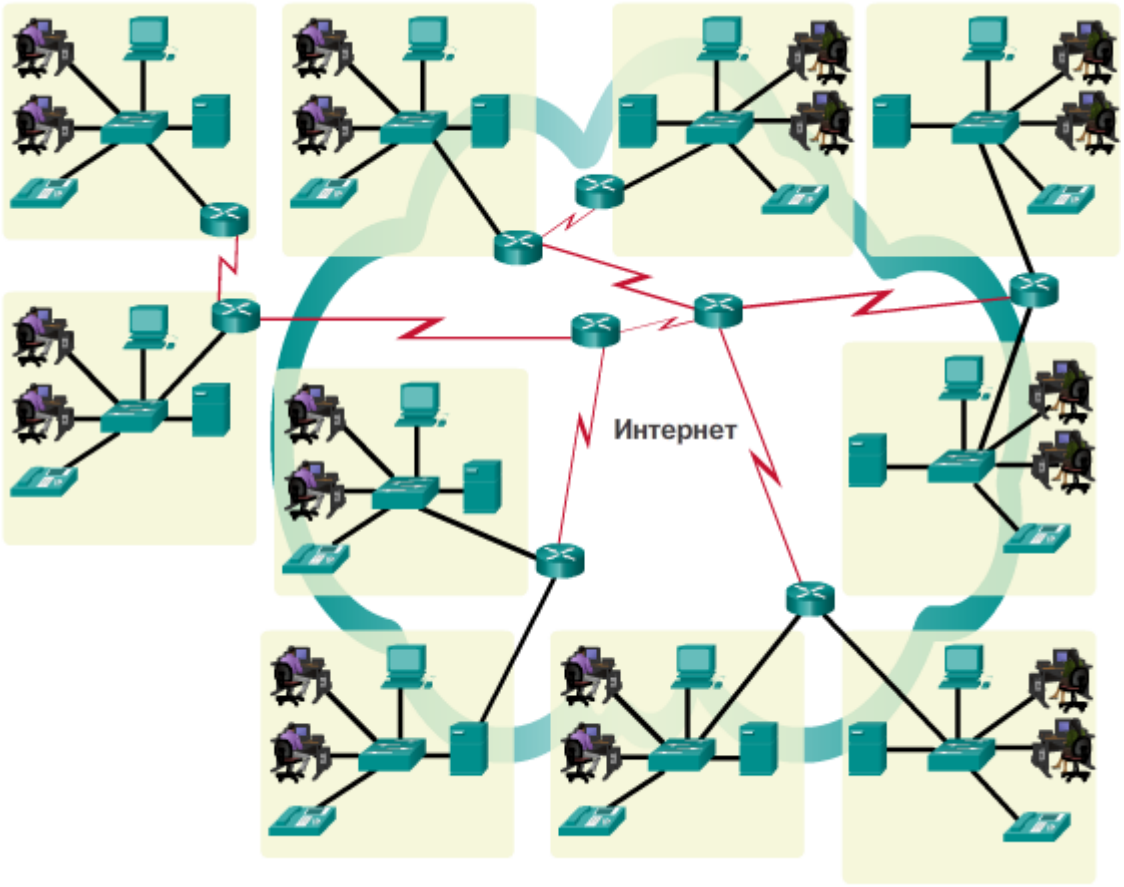

Рисунок 2.11 – Сеть Интернет

2.6.4 Интранет и Экстранет

Два других термина, схожих с термином «Интернет»:

Интранет

Экстранет

Термин «Интранет» (внутренние сети) часто используется для обозначения локальных и глобальных сетей, которые принадлежат организации и доступны только её членам, сотрудникам и прочим авторизованным лицам. Внутренние сети представляют собой объединение сетей, которое обычно доступны только в рамках организации.

Организации могут публиковать во внутренних сетях веб-страницы о внутренних мероприятиях, правилах по технике безопасности, сообщения сотрудников и корпоративные телефонные справочники. Например, в школах могут быть установлены внутренние сети, которые включают данные о расписании занятий, интерактивные учебные программы и дискуссионные форумы. Внутренние сети обычно помогают устранить работу с бумажными документами и ускорить бизнес-процессы. Внутренние сети могут быть

доступны для сотрудников за пределами организации с использованием безопасных подключений к внутренней сети.

Организация может использовать Экстранет (внешние сети) для обеспечения защищённого и безопасного доступа сотрудников, которые работают в различных организациях и которым необходимы данные компании. Примеры сетей экстранет:

Компания, обеспечивающая доступ внешним поставщикам/субподрядчикам.

Больница, где используется система записи к врачам, которые имеют возможность назначать дату приёма пациентов.

Местное управление образования, предоставляющее школам своего района данные о размере бюджета и кадрах.

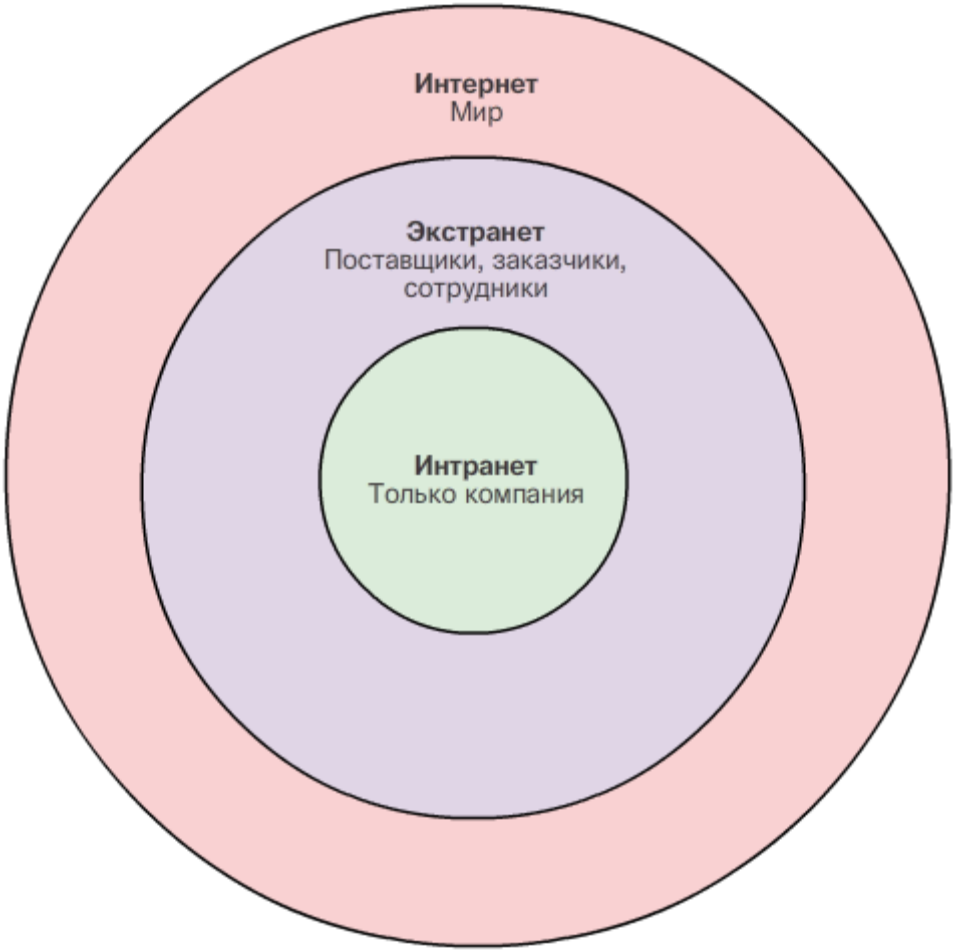

Рисунок 2.12 – Сравнение сетей Интранет, Экстранет и Интернет

2.7 Сеть в качестве платформы

Современные сети непрерывно совершенствуются для удовлетворения потребностей пользователей. Ранее сети передачи данных ограничивались символьно-ориентированным обменом информацией между подключёнными компьютерными системами. Традиционные телефонные, радио- и телевизионные сети были реализованы отдельно от сетей передачи данных. В прошлом каждый из этих сервисов использовал выделенные сетевые ресурсы с различными каналами связи и различными технологиями для передачи определённого сигнала связи. Каждый сервис имел собственный набор правил и стандартов, обеспечивающих успешное сообщение.

Рассмотрим учебное здание, созданное 40 лет назад. В аудитории были проложены кабели для передачи данных, телефонной сети и телевидения. Эти отдельные сети были разрозненные, это означает, что они не могли взаимодействовать друг с другом, как показано на рисунке 2.13.

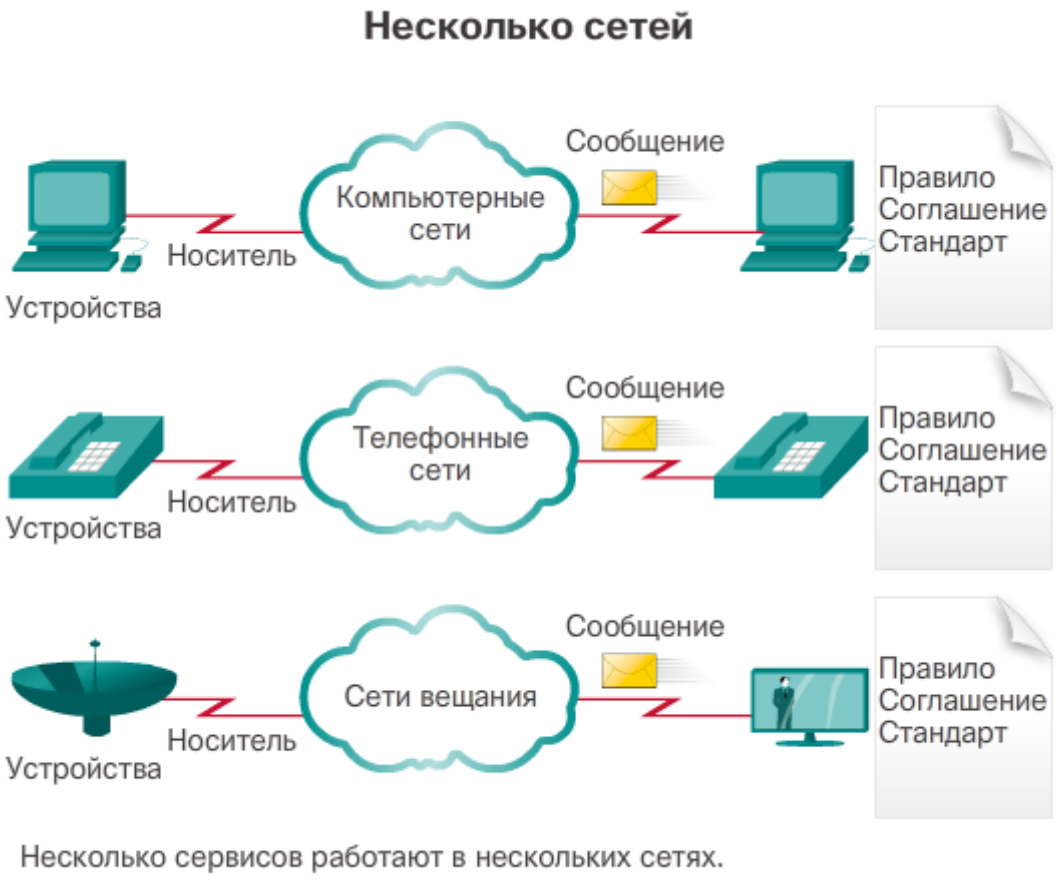

Рисунок 2.13 – Несколько сетей

Развитие технологий позволяет нам объединить эти разные типы сетей в единую платформу, далее именуемую «сошедшаяся сеть». В отличие от

выделенных сетей сошедшиеся системы могут передавать голос, потоковое видео, текст и графические изображения между множеством различных типов устройств по одному и тому же каналу связи и структуре сети, как показано на рисунке 2.14. Ранее бывшие различными формы связи сошлись на общей платформе. Эта платформа предоставляет доступ к широкому диапазону альтернативных и новых способов коммуникации, которые позволяют сотрудникам взаимодействовать друг с другом напрямую практически мгновенно.

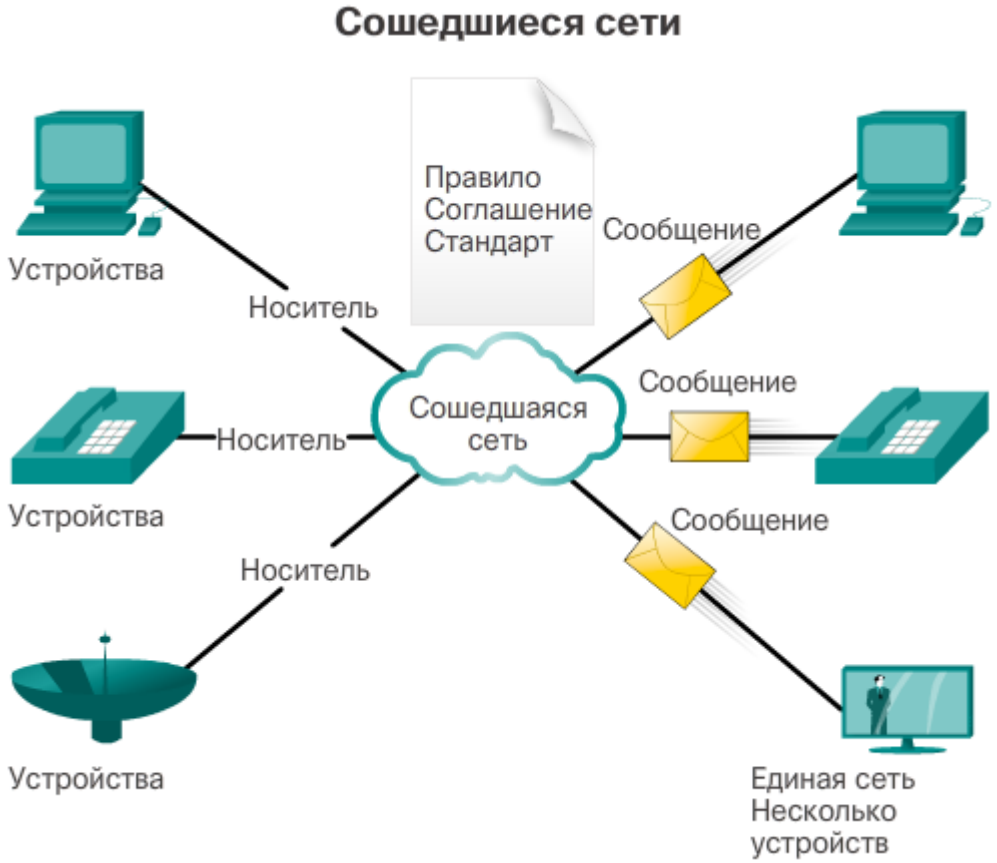

Рисунок 2.14 – Сошедшаяся сеть

В сошедшейся сети по-прежнему существует много контактных точек и много специализированных устройств, таких как персональные компьютеры, телефоны, телевизоры и планшетные компьютеры, но есть общая сетевая инфраструктура. Сетевая инфраструктура использует один и тот же набор правил, соглашения и стандарты реализации.

2.8 Масштабируемые сети

Тысячи новых пользователей и операторов связи подключаются к Интернету каждую неделю. Чтобы Интернет мог поддерживать быстрый рост, ему необходима масштабируемость. Масштабируемую сеть можно быстро

расширить, обеспечив поддержку новых пользователей и приложений без снижения эффективности обслуживания существующих.

Тот факт, что Интернет может расширяться в таких темпах без серьёзного снижения эффективности для отдельных пользователей, является результатом разработки протоколов и технологий, на которых он построен. Интернет имеет иерархическую многоуровневую структуру для адресации, именования, а также для сервисов подключения. В результате сетевому трафику, адресованному местным и региональным сервисам, не требуется проходить через какую-либо центральную точку. Распространённые сервисы могут дублироваться в различных регионах, что позволяет уменьшить трафик на магистралях более высокого уровня.

Масштабируемость также подразумевает способность принимать новые продукты и приложения. Несмотря на то, что не существует ни одной организации, управляющей Интернетом, многие отдельные сети, которые обеспечивают подключение к Интернету, совместно работают над соблюдением принятых стандартов и протоколов. Соблюдение стандартов позволяет производителям аппаратного и программного обеспечения сконцентрироваться на создании новых и модернизации существующих продуктов в области производительности и пропускной способности, при этом новые продукты могут интегрироваться в существующую инфраструктуру и совершенствовать ее.

Текущая архитектура Интернета, несмотря на высокий уровень масштабируемости, не всегда может справиться с растущими потребностями пользователей. Для удовлетворения потребностей в получении новых интернет-приложений и сервисов разрабатываются новые протоколы и структуры адресации.

2.9 Обеспечение безопасности сети

Безопасность

Интернет превратился из жестко контролируемой образовательными и государственными организациями объединенной сети в широкодоступное средство делового и личного общения. В результате изменились требования к безопасности сети. Сетевая инфраструктура, сервисы и данные, содержащиеся в устройствах, подключённых к сетям, представляют важную составляющую

личных и деловых активов. Ущерб для целостности этих ресурсов может привести к серьёзным последствиям, таким как:

Сбои в работе сети, которые не позволяют осуществлять коммуникации и транзакции, что приводит к упущению деловых возможностей

Хищение и использование конкурентами интеллектуальной собственности компании (идеи, патенты или исследования)

Нарушение конфиденциальности и публикация без согласия пользователя его личной или частной информации

Неверное использование и потери личных или корпоративных финансовых средств

Потеря данных, которые требуют существенных трудозатрат на восстановление или являются незаменимыми

Существует два типа проблем безопасности сети, которые необходимо учесть: безопасность сетевой инфраструктуры и безопасность информации.

Обеспечение безопасности инфраструктуры сети включает в себя обеспечение физической безопасности всех устройств, которые необходимы для сетевых подключений, и предотвращение несанкционированного проникновения в управляющее программное обеспечение, выполняемое на них.

Безопасность информации означает защиту данных, содержащихся в пакетах, передаваемых по сети, а также информации, хранящейся на подключённых к сети устройствах. Меры безопасности в сети должны:

Предотвращать несанкционированное раскрытие этой информации

Предотвращать хищение информации

Предотвращать несанкционированное изменение этой информации

Предотвращать отказ в обслуживании (DoS-атака)

Чтобы достичь целей безопасности сети, существует три основных требования, как показано на рисунке 2.15.

Рисунок 2.15 – Требования обеспечения безопасности сети

Обеспечение конфиденциальности данных означает, что только указанные и авторизованные получатели (сотрудники, процессы или устройства) могут получить доступ к данным. Это достигается за счёт надёжной системы аутентификации пользователей, реализации требований к паролям, которые сложно подобрать, а также требований частой смены паролей. Шифрование данных, которые мог бы прочитать только указанный получатель, также входит в конфиденциальность.

Поддержка целостности означает обеспечение уверенности в том, что информация не была изменена в процессе передачи от исходного пункта к месту назначения. Целостность данных может быть нарушена, когда информация повреждена, намеренно или ненамеренно. Целостность данных обеспечивается путем проверки отправителя и использования механизмов проверки того, что пакет не изменился при передаче.

Обеспечение доступности означает средства обеспечения своевременного и надёжного доступа к данным для авторизованных пользователей. Устройства с сетевыми экранами, а также с настольным и серверным антивирусным программным обеспечением позволяют повысить надёжность и устойчивость системы, обнаруживая атаки и защищаясь от них. Создание полностью резервируемых сетевых инфраструктур с малым числом точек отказа может уменьшить последствия этих угроз.

2.10 Тенденции развития сетей

Если посмотреть на то, как Интернет изменил нашу жизнь, трудно поверить, что для большинства людей он появился примерно 20 лет назад. Он действительно изменил способ, которым взаимодействуют сотрудники и организации. Например, прежде чем Интернет стал настолько широко доступным, организации и малый бизнес в большинстве своем полагались на рынок печати, чтобы донести до потребителей информацию о своих продуктах. Компаниям трудно было определить потенциальных заказчиков, поэтому предприятия прибегали к массовым программам печатного маркетинга. Такие программы были дорогостоящими и имели различную эффективность. Сравните с тем, как можно связаться с клиентами теперь. Большинство компаний присутствуют в Интернете, где потребители могут узнать о продуктах, ознакомиться с мнениями других клиентов и оформить заказ прямо на сайте. Сайты социальных сетей устанавливают партнёрство с компаниями для продвижения продуктов и услуг. Блоггеры сотрудничают с компаниями и размещают материалы, которые выделяют из общей массы и рекомендуют продукты и услуги. Большая часть этой рекламы обращена к потенциальному пользователю, а не к массам.

По мере развития новых технологий и появления на рынке новых устройств конечных пользователей предприятия и потребители должны постоянно приспосабливаться к современным изменяющимся условиям. Сеть преобразует связи между пользователями, устройствами и информацией. Существует несколько новых тенденций в развитии сетевых технологий, которые повлияют на организации и потребителей. К некоторым основным тенденциям относятся:

С любого устройства, к любым материалам, любым способом

Совместная работа через Интернет

Видео

Облачные вычисления

Эти тенденции связаны между собой и будут постоянно связаны между собой в ближайшие годы. Следующие несколько тем охватывают эти тенденции более подробно.

2.11 Концепция BYOD («Принеси на работу своё собственное устройство»)

Внедрение концепции BYOD («Принеси на работу своё собственное устройство»)

Концепция доступа с любого устройства к любым материалам любым способом — основная глобальная тенденция, которая требует существенных изменений в том, как устройства используются. Эта популярная тенденция называется «Принеси на работу своё собственное устройство».

«Принеси на работу своё собственное устройство» (Bring Your Own Device, BYOD) значит, что конечные пользователи имеют свободу использования личных инструментов доступа к информации на предприятии или в сети учебного заведения. По мере увеличения популярности потребительских устройств и соответствующего падения цен ожидается, что каждый из сотрудников и учащихся может иметь в личном пользовании самые совершенные вычислительные и сетевые инструменты. Эти персональные средства включают в себя ноутбуки, нетбуки, смартфоны, планшетные ПК и электронные книги. Это могут быть устройства, приобретённые компанией или приобретённые сотрудниками, или и то, и другое.

BYOD означает возможность использования в любом месте любого устройства, независимо от его владельца. Например, в прошлом для доступа к сети учебного заведения или Интернету учащиеся должны были использовать один из компьютеров учебного заведения. Эти устройства рассматривались, как правило, только как средства для работы в классе или в библиотеке. Расширенные возможности подключения с использованием мобильного и удалённого доступа к сети учебного заведения предоставляет учащимся огромную гибкость и более широкий спектр возможностей.

«Принеси на работу своё собственное устройство» (Bring Your Own Device, BYOD) — важная тенденция, которая затронула или затронет каждую организацию ИТ-инфраструктуры.

2.12 Видеосвязь

Другая тенденция в сети, которая является важным фактором в коммуникации и совместной работе, — это видео. Видео используется для обмена информацией, сотрудничества, а также для развлечений. Видеозвонки становятся более популярными, упрощая общение в рамках сети, объединяющей

человечество. Видеовызовы можно совершать из любого места с подключением к Интернету, в том числе из дома или с работы.

Видеовызовы и видеоконференции становятся мощным инструментом для переговоров с заказчиками и ведения бизнеса. Видео — эффективное средство для ведения бизнеса на расстоянии, как локально, так и по всему миру. Сегодня предприятия используют видеосвязь для трансформирования способов ведения бизнеса. Видео помогает предприятиям формировать конкурентные преимущества компании, снижать расходы и уменьшать степень воздействия на окружающую среду за счёт сокращения потребности в командировках. На рисунке 2.16 показана динамика роли видео в коммуникации.

Это изменение привносится в жизнь как компаниями, так и потребителями. Использование видеосвязи становится ключевым требованием для эффективной совместной работы по мере того, как компании расширяются через географические и культурные границы. Пользователи видеосвязи теперь нуждаются в средствах просмотра любых материалов с любого устройства в любой точке мира.

Компании также признают роль видеотехнологий для совершенствования сети, объединяющей людей. Рост объёмов мультимедийных данных, а также их новое применение, вызвали необходимость интеграции аудио и видео во многие виды связи. Аудиоконференции будут продолжать сосуществовать с видеоконференциями. В средства для совместной работы, предназначенные для подключения распределённых сотрудников, интегрируется настольное видео для того, чтобы группы теснее работали вместе.

Существует много причин и преимуществ для внедрения стратегии с использованием видео. У каждой организации свои особенности. Точное сочетание и характер факторов, определяющих внедрение видеосвязи, будут отличаться от организации к организации и по отдельным бизнес-функциям. Маркетинг, например, может сосредоточить усилия на глобализации и быстром изменении вкусов клиентов; в то время как руководители информационных служб могут быть заинтересованы в экономии затрат на командировки сотрудников по всему миру. На рисунке 2 представлены некоторые факторы, побуждающие организации к разработке и внедрению решений по обработке и передаче видео.

Другая тенденция в области видеосвязи — видео по запросу и потоковая передача видео в режиме реального времени. Доставка видео по сети позволяет нам просматривать фильмы и телевизионные программы в желаемое время и в желаемом месте.

Рисунок 2.16 – Динамика роли видео

2.13 Облачные вычисления

Облачные вычисления представляют собой использование вычислительных ресурсов (оборудование и программное обеспечение), которые предоставляются как услуга в сети. Компания использует оборудование и программное обеспечение облачных сервисов и вносит плату за услуги.

Локальным компьютерам больше не нужно выполнять «тяжелую работу» для запуска сетевых приложений. Этим занимается сеть компьютеров, из которых состоит облако. Снижаются требования пользователя к оборудованию и программному обеспечению. Компьютер пользователя должен взаимодействовать с облаком с помощью программного обеспечения, которое может быть браузером, а сети облачных сервисов выполняют другие задачи.

Облачные вычисления — другая глобальная тенденция, которая изменяет способ доступа и хранения данных. Облачные вычисления включают в себя любой сервис по подписке или с оплатой по факту использования в режиме реального времени через Интернет. Облачные вычисления позволяют хранить личные файлы или целый жёсткий диск на серверах в Интернете. Например, приложениями для работы с текстом и для редактирования фотографий можно пользоваться из облака.

Для предприятий облако расширяет ИТ-возможности, не требуя при этом больших капиталовложений в создание новой инфраструктуры, обучение нового персонала или лицензирование нового программного обеспечения. Эти сервисы доступны по запросу и экономично доставляются на любое устройство в любой точке мира без снижения уровня безопасности и ухудшения функциональности.

Термин «облачные вычисления» в действительности означает вычисления, выполняемые в Интернете. Интернет-банк, интернет-магазины и скачивание музыки в Интернете являются наглядными примерами облачных вычислений. Облачные приложения обычно предоставляются пользователю через веб-браузер. Пользователям не нужно предварительно устанавливать на конечные устройства программное обеспечение. Это позволяет большому числу разных типов устройств подключаться к облачным сервисам.

Облачные вычисления предлагают следующие потенциальные преимущества:

Гибкость организации: пользователи могут получить доступ к информации в любое время и в любом месте с помощью веб-браузера.

Оперативность и быстрое развертывание: ИТ-отдел может сконцентрироваться на инструментах по доставке, анализу и совместному использованию информации из баз данных, файлов и от других пользователей.

Снижение затрат на инфраструктуру: технология перемещается с объекта к поставщику облачных услуг, что снижает расходы на оборудование и приложения.

Переориентация ИТ-ресурсов: средства, сэкономленные на оборудовании и приложениях, могут быть использованы по другому назначению.

Создание новых бизнес-моделей: приложения и ресурсы легко доступны, поэтому компании могут быстро реагировать на потребности заказчиков. Это позволяет им проводить стратегию внедрения инноваций и исследовать возможности проникновения на новые рынки.

Существует четыре типа облака, как показано на рисунке 2. Щёлкните каждое облако, чтобы узнать подробные сведения.

2.14 **Центры обработки данных**

Облачные вычисления возможны благодаря центрам обработки данных. Центр обработки данных — это помещение, в котором располагаются компьютерные системы и соответствующие компоненты, такие как:

Резервные соединительные кабели для передачи данных

Высокоскоростные виртуальные серверы (иногда их называют серверными фермами или кластерами)

Резервные системы хранения данных (обычно используется технология сетевой системы хранения данных (SAN))

Источники резервного электропитания

Элементы управления условиями рабочей среды (например, системы кондиционирования воздуха и пожаротушения)

Устройства обеспечения безопасности

Центр обработки данных может занимать одно помещение в здании, один или несколько этажей или всё здание. Современные центры обработки данных используются для облачных вычислений и виртуализации, чтобы сделать эффективной обработку больших массивов данных. Виртуализация, или создание виртуальной версии чего-либо, например, аппаратной платформы, операционной системы (ОС), устройства хранения данных или сетевых ресурсов. В то время как физический компьютер представляет собой фактическое физическое устройство, виртуальная машина состоит из набора файлов и программ, работающих на физической системе. В отличие от многозадачности, состоящей в том, чтобы запустить несколько программ на одной и той же ОС, при использовании виртуализации несколько различных операционных систем работают параллельно на одном ЦП. Подобная схема значительно уменьшает затраты на администрирование и накладные расходы.

Центры обработки данных обычно дорого создавать и обслуживать. По этой причине только крупные организации используют специально созданные центры обработки данных для размещения корпоративных данных и сервисов для пользователей. Например, крупное медицинское учреждение может иметь собственный центр обработки данных, где истории болезней пациентов ведутся в электронном виде. Небольшие организации, которые не имеют собственного центра обработки данных, могут снизить общую стоимость владения за счёт выделения сервера и сервисов хранения данных в центре обработки данных более крупной организации.

Здесь представлен видеоролик о растущем использовании сервисов центров обработки данных и облачных вычислений.

ГЛАВА 3 МЕТОДИЧЕСКИЕ УКАЗАНИЯ

3.1 Общие сведения

1. Учебный стенд представляет собой коммутационный шкаф с

установленным сетевым оборудованием, 4 учебных рабочих места и комплекта кабелей (коммутационных патч-кордов, консольных кабелей).

2. В коммутационном шкафу установлены:
   - маршрутизатор Cisco 2811- 1 шт
   - маршрутизатор Cisco 2821- 2 шт;
   - коммутатор Cisco Catalyst 3560 - 1 шт;
   - коммутатор Cisco Catalyst 2960 - 2 шт;
   - неуправляемый коммутатор D-link DSG-1005 - 4 шт
   - низкоуровневый анализатор пакетов Ethernet - 1 шт
   - коммутационная панель.

3. Учебное рабочее место (WS) состоит из системного блока ПЭВМ, с установленной на ней операционной системой семейства Linux Mint, монитора, клавиатуры, манипулятора «мышь».

4. На рабочих станциях установлено следующее программное обеспечение:
   - анализатор сетевого трафика Wireshark;
   - среда удаленного управления Putty;
   - файловый менеджер MC;
   - генератор трафика iperf;
   - сервер (клиент Samba).
   - tftp-сервер, tftp-клиент;
   - виртуальная машина virtual-box;
   - nfs клиент и сервер nfs-common.

5. На рабочей станции 1 (WS 1) в дополнение к п.4 установлена виртуальная машина VirtualBox с образами виртуальных машин Windows 7 и Linux SLES. На виртуальной машине Windows 7 установлены:
   - сервер управления SNMP протоколом powersnmp_free_manager.exe
   - сервер WinRadius.

   На виртуальной машине Linux SLES установлены:
   - HTTP-сервер Apache
   - DNS-сервер
   - FTP-сервер
   - сервер Samba

6. Базовые настройки аппаратуры стенда представлены в таблице 1.

Таблица 3.1 - Базовые настройки PC

Устройство	IP-адрес	Пользователь	Пароль
WS 1 (eth1)	192.168.0.101	ws1	123456
WS 1 (eth2)	192.168.0.102		123456
WS 1 (eth3)	192.168.0.103		123456
WS 2 (eth1)	192.168.0.104	ws2	123456
WS 4 (eth3)	192.168.0.112	ws4	123456
Web-сервер	192.168.0.200		
FTP- сервер	192.168.0.200		
DNS- сервер	192.168.0.200		
TFTP-сервер	192.168.0.210		
WS 1 (Windows)	192.168.0.210	ws1sles1	123456
Ethernet контроллер	192.168.0.222		

7. В качестве ОС Windows используется неактивированная, пробная версия операционной системы Windows 7.

3.2 Лабораторная работа №1. Знакомство с учебным стендом

1. Включите ПЭВМ (рабочие станции, Work Station (WS), расположенные на рабочих местах.
2. Загрузите операционные системы, установленные на рабочих станциях (WS).
3. Изучите программное обеспечение, установленное на WS.
4. Изучите расположение сетевых устройств в коммутационной стойке и прилагаемые к нему принадлежности.
5. Соедините WS 1 в локальную сеть с использованием коммутатора через гнезда коммутационной панели, согласно топологии (рисунок 3.1).

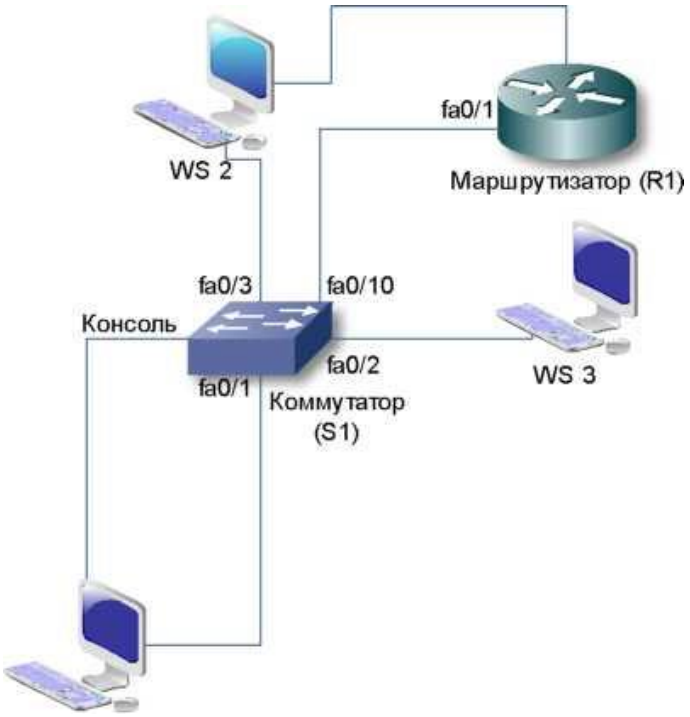

Рисунок 3.1 - Топология сети

6. Настройте сетевые адреса WS в соответствие с таблицей адрессации (таблица 3.2).

Таблица 3.2 - Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Примечание
Маршрутизатор (R1)	Fa0/1	192.168.1.100	255.255.255.0	
Cisco коммутатор (S1)				
WS 1	NIC	192.168.1.10	255.255.255.0	
WS 2	NIC	192.168.1.11	255.255.255.0	
WS 3	NIC	192.168.1.12	255.255.255.0	

7. С каждой WS проверьте доступность соседних WS командой ping. Для этого откройте на рабочем столе WS откройте терминальный режим и в командной строке введете

ping 192.168.0.11

8. Соедините консольным кабелем с COM-порту WS 1 и консольный порт коммутатора.

9. На WS 1 запустите программу консольного управления, например putty. Для этого используйте команду действия от суперпользователя sudo в терминальном режиме.

sudo putty

10. По запросу введите пароль суперпользователя (по умолчанию «123456»)
11. В программе putty выберите режим управления по консоли «Consol» и установите связь с сетевым устройством.
12. Включите коммутатор подключив сетевой провод к розетке 220В. Пронаблюдайте порядок загрузки устройства «Cisco».
13. Просмотрите команды доступные в пользовательском режиме
    Switch>?
14. Перейдите в привилегированный режим командой *enable*
    Switch#
15. Просмотрите команды доступные в привилегированном режиме
    Switch#?
16. Перейдите в режим глобальной конфигурации. Для этого введите команду configure terminal
    Switch#configure terminal
    Switch(config)#
17. Просмотрите команды доступные в режим глобальной конфигурации
    Switch(config)#?
18. Соедините консольным кабелем с COM-портом WS2 и консольный порт маршрутизатора.
19. На WS2 запустите программу консольного управления, например putty. Для этого используйте команду действия от суперпользователя sudo в терминальном режиме.
    sudo putty
20. По запросу введите пароль суперпользователя (по умолчанию «123456»)
21. В программе putty выберите режим управления по консоли «Consol» и установите связь с сетевым устройством.
22. Включите маршрутизатор тумблером питания. Пронаблюдайте порядок загрузки устройства «Cisco».
23. Просмотрите команды доступные в пользовательском режиме
    Router>?
24. Перейдите в привилегированный режим командой enable
    Router#
25. Просмотрите команды доступные в привилегированном режиме
    Router#?
26. Перейдите в режим глобальной конфигурации. Для этого введите команду configure terminal
    Router#configure terminal
    Router(config)#
27. Просмотрите команды доступные в режим глобальной конфигурации
    Router(config)#?
28. Сравните доступные команды маршрутизатора и коммутатора в различных режимах.
29. Сделайте соответствующие выводы по работе.
30. Выключите сетевые устройства и WS, приведите рабочее место в исходное состояние.

3.3 Лабораторная работа №2. Первоначальная настройка сетевых устройств

Соберите топологию сети в соответствии с рисунком 3.2. Подсоедините консольные кабели к устройствам, показанным на топологической схеме. Отразите топологию сети в отчете лабораторной работы.

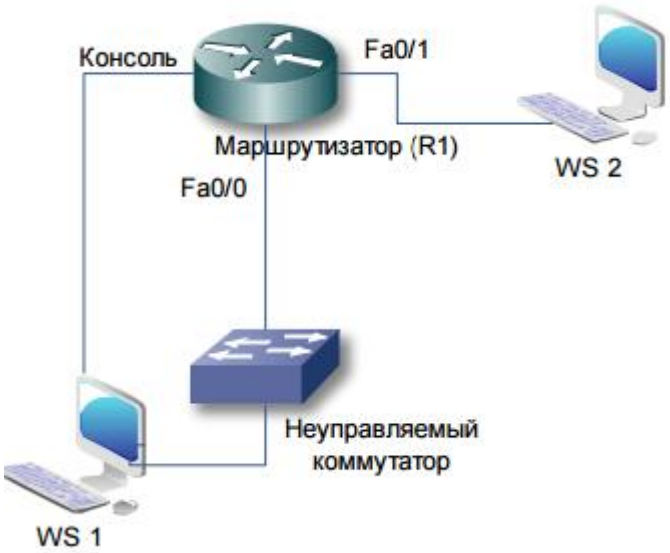

Рисунок 3.2 – Топология сети

1. Включите и загрузите операционные системы (ОС) на рабочих станциях (WS).
2. Включите все сетевые устройства и дождитесь завершения процесса загрузки программного обеспечения.
3. Подключитесь к маршрутизатору. Для этого на WS откройте терминальную сессию и запустите от имени суперпользователя программу Putty. В ней выберите подключение по последовательному порту «Serial» и войдите в привилегированный режим EXEC с помощью команды *enable*:

Router> enable
Router#

4. Удалите файл загрузочной конфигурации из NVRAM. Для этого введите команду *erase startup-config*, чтобы удалить загрузочную конфигурацию из энергонезависимого ОЗУ (NVRAM).

Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]

Erase of nvram: complete

Router#

5. Перезагрузите маршрутизатор, выполнив команду *reload*, чтобы удалить устаревшую информацию о конфигурации из памяти. По запросу перезагрузки нажмите клавишу Enter, чтобы подтвердить перезагрузку. Чтобы прервать процесс перезагрузки, нажмите любую клавишу.

Router# reload

6. После перезагрузки маршрутизатора появится запрос о входе в диалоговое окно начальной конфигурации. Введите no и нажмите клавишу Enter.

Router>

Сетевое устройство готово к начальному конфигурированию.

7. Отметьте команды IOS, используемые при настройке, а также реакцию сетевого устройства в отчете лабораторной работы.

8. Изучите сведения о версии ОС Cisco IOS на маршрутизаторе, используя команду *show version*. Команду и результат ее выполнения отметьте в бланке лабораторной работы.

Switch# show version

9. Изучите сведения об имеющихся на маршрутизаторе сетевых интерфейсах, используя команду *show interfaces*. Команду и результат ее выполнения отметьте в бланке лабораторной работы.

Switch# show version

10. Изучите флеш-память сетевого устройства. Выполните одну из следующих команд, чтобы изучить содержимое флеш-каталога. Команду и результат ее выполнения отметьте в бланке лабораторной работы.

Switch# show flash

Switch# dir flash:

11. Выполните инициализацию и перезагрузку коммутатора. Для этого соберите топологию сети в соответствии с рисунок 3.3.

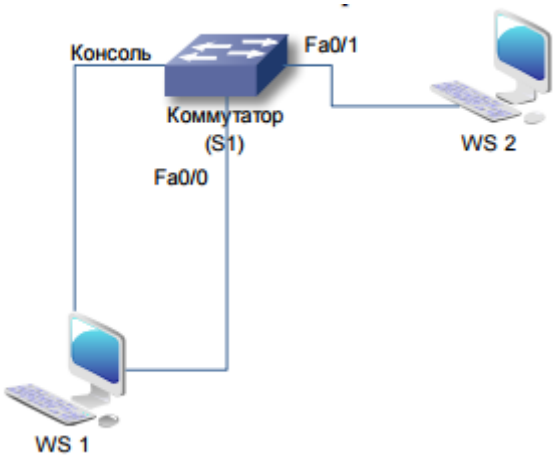

Рисунок 3.3 - Топология сети

12. Подключитесь к коммутатору с помощью консольного подключения и войдите в привилегированный режим EXEC.

Switch> enable

13. Определите наличие ранее созданных виртуальных локальных сетей

(VLAN). Воспользуйтесь командой *show flash*, чтобы определить, были ли созданы сети VLAN на коммутаторе:

Switch# show flash

14. Если во флеш-памяти обнаружен файл *vlan.dat*, удалите его.

Switch# delete vlan.dat

Delete filename [vlan.dat]?

Будет предложено проверить имя файла. На данном этапе можно изменить имя файла или нажать клавишу Enter, если правильное имя уже введено. При появлении запроса на удаление этого файла нажмите клавишу Enter, чтобы подтвердить удаление.

15. Удалите файл загрузочной конфигурации. Для этого введите команду *erase startup-config*, чтобы удалить файл загрузочной конфигурации из NVRAM. При появлении запроса на удаление конфигурационного файла нажмите клавишу Enter, подтверждающую удаление.

Switch# erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK]

Erase of nvram: complete

Switch#

16. Перезагрузите коммутатор, чтобы удалить устаревшую информацию о конфигурации из памяти. При необходимости перезагрузки коммутатора нажмите клавишу Enter, чтобы продолжить перезагрузку.

Switch# reload

Proceed with reload? [confirm]

System configuration has been modified. Save? [yes/no]: no

17. После перезагрузки коммутатора появится запрос о входе в диалоговое окно начальной конфигурации. Введите no в окне запроса и нажмите клавишу Enter.

Would you like to enter the initial

configuration dialog? [yes/no]: no

Switch>

Сетевое устройство готово к начальному конфигурированию.

18. Отметьте команды IOS, используемые при настройке в предыдущих пунктах, а также реакцию сетевого устройства в отчете лабораторной работы.

19. Изучите IP-свойства интерфейса SVI сети VLAN 1. Для этого введите команду show ip interface vlan 1. Команду и результат ее выполнения отметьте в бланке лабораторной работы.

Switch# show ip interface vlan1

20. Изучите сведения о версии ОС Cisco IOS на коммутаторе, используя команду *show version*. Команду и результат ее выполнения отметьте в бланке лабораторной работы.

Switch# show version

21. Изучите свойства по умолчанию интерфейса FastEthernet, который используется PC. Для этого введите команду show interface «порт интерфейса», например show interface fa0/6. Команду и результат ее выполнения отметьте в бланке лабораторной работы.

Switch# show interface fa0/6

22. Изучите параметры сети VLAN по умолчанию на коммутаторе, используя команду show vlan. Команду и результат ее выполнения отметьте в бланке лабораторной работы.

Switch# show vlan

23. Изучите флеш-память сетевого устройства. Выполните одну из следующих команд, чтобы изучить содержимое флеш-каталога. Команду и результат ее выполнения отметьте в бланке лабораторной работы.

Switch# show flash Switch#

dir flash:

31. Сделайте соответствующие выводы по работе.

32. Выключите сетевые устройства и WS, приведите рабочее место в исходное состояние.

3.4 Лабораторная работа №3. Администрирование коммутаторов

Соберите топологию сети в соответствие с рисунком 3.4.

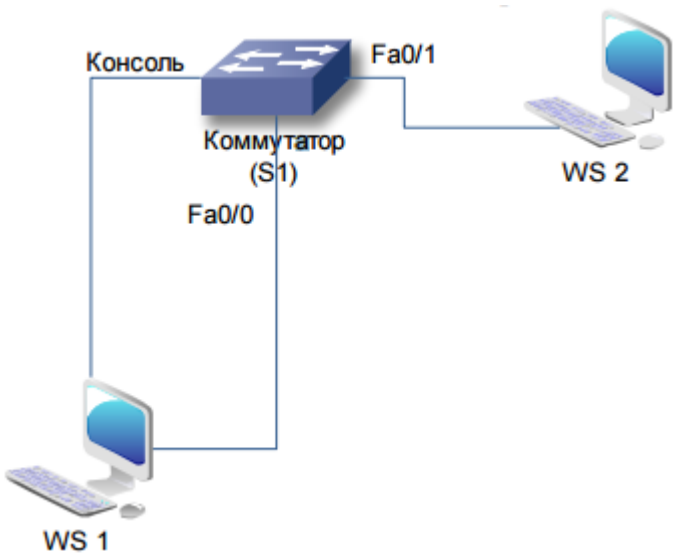

Рисунок 3.4 - Топология сети

1. Создайте таблицу адресации сети по примеру, указанному в таблице 3.3 Отразите ее в отчете лабораторной работы.

Таблица 3.3 - Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Cisco коммутатор (S1)	VLAN 99	192.168.1.2	255.255.255.0	192.168.1.1
WS 1	NIC	192.168.1.10	255.255.255.0	192.168.1.1
WS 2	NIC	192.168.1.20	255.255.255.0	192.168.1.1

2. Включите и загрузите операционные системы (ОС) на рабочих станциях (WS)

3. На WS запустите TFTP-сервер и проверьте его работоспособность Отразите в отчете лабораторной работы порядок запуска TFTP-сервера.

4. Сконфигурируйте основные настройки сетевых устройств. Конфигурирование заключается в назначении имени коммутатора, настройки возможности удаленного управления. Задайте коммутатору имя узла. Рекомендуется в качестве имени использовать название сетевого устройства и порядковый номер его расположения в стойке оборудования, например S1 или Switch1. Для этого в режиме глобальной конфигурации введите следующие команды:

```
Switch(config)# hostname S1
S1(config)#
```

Настройте шифрование пароля. В качестве секретного пароля для доступа в привилегированный режим задайте легкозапоминающуюся комбинацию, например «class»

```
Sl(config)# service password-encryption
S1(config)# enable secret class
```

Запретите нежелательный поиск в DNS.

```
S1(config)# no ip domain-lookup
S1(config)#
```

Настройте баннер MOTD (сообщение). В качестве сообщения рекомендуется использовать напоминание о названии сетевого устройства и порядковый номер его расположения в стойке оборудования, например S1 или Switchl.

```
S1(config)# banner motd
```

Проверьте настройки доступа, переключаясь между режимами.

Вернитесь из пользовательского режима в привилегированный режим. При запросе пароля введите ранее заданный пароль.

```
S1> enable
Password:
S1#
```

5. Согласно конфигурации коммутатора по умолчанию управление коммутатором должно осуществляться через VLAN 1. Однако в базовой конфигурации коммутатора не рекомендуется назначать VLAN 1 в качестве административной VLAN. Для административных целей используйте, например VLAN 100. Создайте на коммутаторе новую VLAN 100. Настройте на внутреннем виртуальном интерфейсе (SVI) VLAN 100 и IP-адрес коммутатора, например 192.168.1.2 с маской подсети 255.255.255.0. Для назначения коммутатору IP-адреса SVI для удалённого управления необходимо войти в режим глобальной конфигурации.

```
S1# configure terminal
S1(config)# vlan 100
S1(config-vlan)# exit
```

S1(config)# interface vlan100
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit

6. Ассоциируйте все пользовательские порты с VLAN 100.

S1(config)#interface range fa0/1 – 24, g0/1 – 2
S1(config-if-range)# switchport access vlan 100
S1(config-if-range)# exit

7. Убедитесь, что все пользовательские порты находятся в сети VLAN 100, выполнив команду *show vlan brief*.

S1# show vlan brief

8. Настройте IP-шлюз по умолчанию для коммутатора S1. Например, интерфейс LAN маршрутизатора, работающего в качестве шлюза равен 192.168.1.1. Данный IP-адрес необходимо настроить в качестве шлюза по умолчанию для коммутатора.

S1(config)# ip default-gateway 192.168.1.1

9. Чтобы консольные сообщения не прерывали выполнение команд, используйте параметр *logging synchronous*.

S1(config)# line con 0
S1(config-line)# password 123456
S1(config-line)# login
S1(config-line)# logging synchronous
S1(config-line)# exit

Отметьте команды IOS, используемые при настройке сетевого устройства в отчете лабораторной работы.

10. Настройте сетевые интерфейсы WS согласно адресному плану сети.
11. При помощи команды ping проверьте доступность устройств с сети. Результат отметьте в отчете лабораторной работы.
12. Настройте возможность конфигурирования сетевых устройств с помощью протокола telnet. Для этого сконфигурируйте каналы виртуального соединения для удалённого управления (vty), чтобы коммутатор разрешил доступ через Telnet с использованием пароля «cisco».

S1(config)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# end

Отметьте команды IOS, используемые при настройке сетевого устройства, в отчете лабораторной работы.

13. На WS войдите в режим терминала от имени суперпользователя и запустите сеанс протокола telnet командой

sudo telnet ^ip-адрес сетевого устройства>

14. Сохраните созданную конфигурацию на TFTP-сервере под именем start. Для этого используйте следующие команды:

copy runung-config tftp

15. По запросу введите ip-адрес сетевого устройства, где запущен TFTP-сервер и имя файла, в который запишется текущая конфигурация сетевого

устройства (для простоты рекомендуем имя файла «start»).
16
16. Зайдите в папку, указанную в качестве хранилища на TFTP-сервере и проверьте наличие файла с конфигурацией сетевого устройства.
17. Сохраните созданную конфигурацию во флеш-памяти сетевого устройства. Для этого используйте следующие команды:

copy runung-config startup-config.

18. Перезагрузите сетевое устройство и проверьте возможность доступа к нему через консоль управления и по протоколу telnet.
19. Удалите стартовую конфигурацию сетевого устройства и перезагрузите устройство.
20. Загрузите с TFTP-сервер стартовую конфигурацию сетевого устройства.
21. Сохраните загруженную конфигурацию во флеш-памяти сетевого устройства.
22. Перезагрузите сетевое устройство и проверьте возможность доступа к нему через консоль управления и по протоколу Telnet.
23. Выключите сетевые устройства и WS, приведите рабочее место в исходное состояние. Сделайте соответствующие выводы по работе.
24. Выключите сетевые устройства и WS, приведите рабочее место в исходное состояние

3.5 Лабораторная работа №4. Управление сетью с помощью протокола SNMP

Изучите методику по настройке сервера SNMP-протокола в соответствующих разделах брошюры «Примеры настройки программного обеспечения стенда».

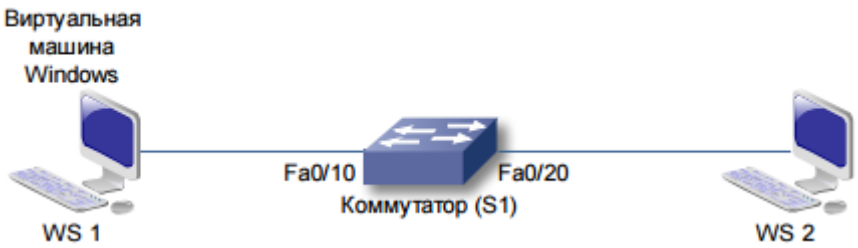

Рисунок 3.5 – Топология сети

1. Соберите топологию сети в соответствие с рисунком 3.5

2. Создайте таблицу адресации сети по примеру, указанному в таблице 4.1. Отразите ее в отчете лабораторной работы.

Таблица 3.4 - Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Cisco коммутатор (S1)	VLAN 99	192.168.1.2	255.255.255.0	192.168.1.1
WS 1	NIC	192.168.1.10	255.255.255.0	192.168.1.1
WS 2	NIC	192.168.1.100	255.255.255.0	192.168.1.1

3. Включите и загрузите операционные системы (ОС) на рабочих станциях (WS)
4. На WS запустите TFTP-сервер и проверьте его работоспособность.
5. Настройте базовые параметры коммутатора.
6. На WS 1 запустите виртуальную машины с ОС Windows. В качестве программы SNMP управления используйте *powersnmp_free_manager.exe*.
7. Настройте коммутатор для поддержки SNMP-протокола. Для этого выполните следующие команды:

S1# configure terminal
S1(config)# sdm prefer lanbase-routing
S1(config)# end S1# reload
S1# configure terminal
S1(config)# snmp-server community ciscolab ro SNMP_ACL
S1(config)# snmp-server host 192.168.1.100 version 2c ciscolab
S1(config)# snmp-server enable traps S1(config)# ip access-list standard SNMP_ACL S1(config-std-nacl)# permit 192.168.1.100

8. На виртуальной машине запустите среду управления протоколом SNMP. Используя рекомендации, указанные в соответствующих разделах брошюры «Примеры настройки программного обеспечения стенда», настройте доступ к коммутатору.
9. При настроенных в сети SNMP-агентах программа PowerSNMP Free Manager получает уведомления от сетевых устройств. Если уведомления не приходят, следует установить принудительно отправку уведомления SNMP, введя команду copy run start на коммутаторе S1.
10. Настройте маршрутизатор R1 в качестве агента SNMP. Используйте те же команды, которые вы использовали для настройки коммутатора.
11. После завершения настройки маршрутизатора проверьте наличие уведомлений SNMP с его IP-адреса в окне «Traps» (Прерывания). Результат отметьте в бланке лабораторной работы.
12. Добавьте маршрутизатор R1 в качестве агента SNMP.
13. Подключите к коммутатору WS2.
14. Проследите сообщения в программе PowerSNMP Free Manager. Результат отметьте в бланке лабораторной работы.

15. Отключите коммутатор от локальной сети.
16. Проследите сообщения в программе PowerSNMP Free Manager. Результат отметьте в бланке лабораторной работы.
17. Загрузите с TFTP-сервера стартовую конфигурацию сетевых устройств.
18. Сохраните загруженные конфигурации во флеш-память сетевых устройств.
19. Перезагрузите сетевые устройства и проверьте возможность доступа к ним через консоль управления и по протоколу Telnet.
20. Выключите сетевые устройства и WS, приведите рабочее место в исходное состояние. Сделайте соответствующие выводы по работе.

4 ТЕХНИКО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ ПРОЕКТА

4.1 Описание работы и обоснование необходимости

Тема данной дипломной работы «Разработка комплекса лабораторных работ по дисциплине «Компьютерные сети»».

Целью данного проекта является разработать 7 лабораторных работ по направлению сетевых технологии, коммутации и маршрутизации данных передаваемых в компьютерных сетях.

В данном разделе приводится рассмотрение экономической составляющей реализации данной работы, отражающей временные, трудовые и финансовые затраты на проект.

4.2 Трудовые ресурсы, используемые в работе

В данной дипломной работе используется интеллектуальный труд. В работе задействованы:

- руководитель;
- инженер - разработчик;

Таблица 4.1 – Данные о работниках, задействованных в проекте и их заработная плата

Исполнитель	Количество человек	Заработная плата, тенге
Руководитель	1	60 000
Инженер - разработчик	1	170 000
Итого	**4**	**230 000**

4.3 Оборудование и программное обеспечение, используемое в работе

Общая стоимость расходов на оборудование составляет 133214 тенге.

Программное обеспечение, необходимое для реализации данного проекта, а именно программа для создания и тестирования прототипов сети, Cisco Packet Tracer имеет бесплатную форму распространения, для образовательных учреждений, в которых действует Сетевая Академия Cisco.

Данные по количеству каждого вида оборудования и стоимости представлены в таблице 4.2.

Т а б л и ц а 4 . 2 – Используемое оборудование

Наименование материала	Единицы измерения	Количество	Сумма в тенге (Без НДС)
Ноутбук Samsung Intel(R) Core ™ i3 2.13 GHz/RAM 4Gb/HDD 500Gb	штук	1	125000
Мышка Razer Coperhead Zx7	штук	1	8214
Packet Tracer версии 6.1.1	штук	1	беспл.
Принтер	штук	1	18000
Итого:			151214

4.4 Расчет стоимости разработки ПО

Себестоимость разработки проекта определяется по следующей формуле

$$С = ФОТ + С_н + А + С_{эл} + Н \quad (4.1)$$

где ФОТ – фонд оплаты труда;
$С_н$ – социальный налог;

А – амортизационные отчисления;
$С_{эл}$– расходы на электроэнергию;

Н – накладные расходы.

4.5 Сроки реализации проекта

Разработка комплекса лабораторных работ по дисциплине «Компьютерные сети» включает следующие этапы (таблица 4.3):

- 1 этап: Постановка задачи
- 2 этап: Разработка задания
- 3 этап: Написание методических указаний
- 4 этап: Апробирование лабораторных работ

- 5 этап: Проверка работоспособности комплекса лабораторных работ
- 6 этап: Оформление отчетов

Таблица 4.3 – Этапы и сроки реализации проекта

Перечень работ		**Недели от начала работ**									
		1	2	3	4	5	6	7	8	9	10
1 этап	Постановка задачи	■									
	Обзор и анализ технологий	■									
	Подбор и изучение литературы		■								
2 этап	Разработка задания		■	■							
	Изучение функции оборудования			■							
	Рассмотрение команд настройки			■							
3 этап	Написание методических указаний			■	■						
	Порядок выполнения работы				■						
4 этап	Апробирование лабораторных работ				■	■					
	Конфигурирование оборудования в соответствии с заданием					■	■	■			
5 этап	Проверка работоспособности комплекса лабораторных работ							■			
	Тестирование настроек								■		
	Отладка недочетов									■	
6 этап	Оформление отчетов									■	■

4.5.1 Расчет затрат на оплату труда

Для расчета затрат на заработную плату необходимы следующие данные:

– численность задействованного персонала;

– среднемесячная заработная плата каждого работника;

– длительность разработки проекта и каждого вида выполняемых работ;

– трудоемкость.

В процессе разработки данного программного обеспечения участвует 4 человека.

Месячная заработная плата сотрудников:

- инженер - разработчик – 170 000 тенге;
- руководитель – 60000 тенге;

Заработную плату за один час рассчитаем по формуле

$$D = \frac{ЗПм}{Др \cdot Чр} \qquad (4.2)$$

где $ЗПм$ – ежемесячный размер заработной платы;

$Др$ – количество рабочих дней в месяце (21 рабочий день);

$Чр$ – количество часов рабочего дня (при 8 часовом рабочем дне).

1) Заработная плата инженера - разработчика за один час составляет:

$$D = \frac{170000}{21 \cdot 8} = \frac{170000}{168} = 1011{,}9 \text{ тенге/час}$$

2) Заработная плата руководителя за один час составляет:

$$D = \frac{60000}{21 \cdot 8} = \frac{60000}{168} = 357{,}14 \text{ тенге/час}$$

Длительность цикла в днях по каждому виду работ укрупнено, определяем по формуле

$$t_n = T / q_n \cdot z \cdot K, \qquad (4.3)$$

где T – трудоемкость этапа, норма-час;

q_n – количество исполнителей по этапу;

z – продолжительность рабочего дня, z = 8 часов;

K – коэффициент выполнения норм времени, K = 1,1.

Полученная величина t_n округляется в большую сторону до целых дней.

$t_1 = \frac{20}{1 \cdot 8 \cdot 1.1} = \frac{20}{8.8} \approx 3$ дн; Руководитель: постановка задачи;

$t_2 = \frac{10}{1 \cdot 8 \cdot 1.1} = \frac{10}{8.8} \approx 2$ дн; Руководитель: разработка задания;

$t_3 = \frac{20}{1 \cdot 8 \cdot 1.1} = \frac{20}{8.8} \approx 3$ дн; Руководитель: подбор и изучение литературы;

$t_4 = \frac{20}{1 \cdot 8 \cdot 1.1} = \frac{20}{8.8} \approx 3$ дн; Инженер - разработчик: написание методических указаний;

$t_5 = \frac{5}{1 \cdot 8 \cdot 1.1} = \frac{5}{8.8} \approx 1$ дн; Инженер - разработчик: описание порядка выполнения работы;

$t_6 = \frac{10}{1 \cdot 8 \cdot 1.1} = \frac{10}{8.8} \approx 2$ дн; Инженер - разработчик: изучение функции оборудования;

$t_7 = \frac{28}{1 \cdot 8 \cdot 1.1} = \frac{28}{8.8} \approx 4$ дн; Инженер - разработчик : рассмотрение команд настройки;

$t_8 = \frac{28}{1 \cdot 8 \cdot 1.1} = \frac{28}{8.8} \approx 4$ дн; Инженер - разработчик: постановка лабораторных работ;

$t_9 = \frac{80}{1 \cdot 8 \cdot 1.1} = \frac{80}{8.8} \approx 10$ дн; Инженер - разработчик: конфигурирование оборудования в соответствии с заданием;

$t_{10} = \frac{20}{1 \cdot 8 \cdot 1.1} = \frac{20}{8.8} \approx 3$ дн; Инженер - разработчик: проверка работоспособности комплекса лабораторных работ;

$t_{11} = \frac{38}{1 \cdot 8 \cdot 1.1} = \frac{38}{8.8} \approx 5$ дн; Инженер - разработчик: тестирование настроек;

$t_{12} = \frac{20}{1 \cdot 8 \cdot 1.1} = \frac{20}{8.8} \approx 3$ дн; Инженер - разработчик: отладка недочетов;

$t_{13} = \frac{17}{1 \cdot 8 * 1.1} = \frac{17}{8.8} \approx 2$ дн; Инженер - разработчик: проверка и сдача отчета;

$t_{14} = \frac{28}{1 \cdot 8 * 1.1} = \frac{28}{8.8} \approx 4$ дн; Руководитель: проверка и сдача отчета.

Затраты по основной з/плате составляют 297011,4 тенге.

Сводные результаты расчета затрат на основную заработную плату работников, задействованных в разработке комплекса лабораторных работ, предоставлены в таблице 4.4.

Т а б л и ц а 4 . 4 – Сводные результаты расчета затрат на основную заработную плату.

№	Наименование содержания работы	Исполнитель	Трудоемкость		Длительность цикла, дни	Заработанная плата за час работы, тенге	Сумма заработной платы, тенге
			Нормы часы	% от общей трудоемкости			
1	2	3	4	5	6	7	8
1	Постановка задачи	Руководитель	20	4,95	3	357	7140
2	Разработка задания	Руководитель	10	2,475	2	357	3570
3	Подбор и изучение лит.	Руководитель	20	4,95	3	357	7140
4	Написание метод. указаний	Инженер - разработчик	20	4,95	3	1011,9	20238
5	Описание порядка выполнения работы	Инженер - разработчик	5	1,23	1	1011,9	5059,5
6	Изучение функции оборудования	Инженер - разработчик	10	2,475	2	1011,9	10119
7	Рассмотрение команд настройки	Инженер - разработчик	28	6,93	4	1011,9	28333,2
8	Постановка лаб. работ	Инженер - разработчик	28	6,93	4	1011,9	28333,2

9	Конфигурирование оборудования в соответствии с заданием	Инженер - разработчик	80	19,8	10	1011,9	80952
10	Проверка работоспособности комплекса лаб. работ	Инженер - разработчик	20	4,95	3	1011,9	20238
11	Тестирование настроек	Инженер - разработчик	38	9,405	5	1011,9	38452,2
12	Отладка недочетов	Инженер - разработчик	20	4,95	3	1011,9	20238
13	Проверка и сдача отчета	Инженер - разработчик	17	4,207	2	1011,9	17202,3
14	Проверка и сдача отчета	Руковод.	28	6,93	3	357	9996
	Итого	**-**	**344**	**85,15**	**48**	**-**	**297011,4**

Дополнительная заработная плата составляет 10 % от основной заработной платы и рассчитывается по формуле:

$$З_{доп} = ФОТ \cdot 0,1 \quad (4.4)$$

$З_{доп} = 297011,4 \cdot 0,1 = 29701,14$ тенге

Таким образом, суммарный фонд оплаты труда работников составит:

ФОТ = 297011,4+ 29701,14 = 326712,54 тенге

4.5.2 Расчет затрат по социальному налогу

Согласно разделу 11 «Социальный налог» статья 317 «Ставки налога» НК РК юридические лица — резиденты Республики Казахстан, а также нерезиденты, осуществляющие деятельность в Республике Казахстан через постоянное учреждение, филиалы и представительства, уплачивают социальный налог в размере 11 % от начисленных доходов.

Социальный налог рассчитывается по формуле

$$С_н = (ФОТ - ПО) \cdot 11\ \% \quad (4.5)$$

где ФОТ – фонд оплаты труда,

ПО – пенсионные отчисление;
Пенсионные отчисления вычисляются по формуле

$$ПО = ФОТ \cdot 10\,\% \qquad (4.6)$$

$ПО = 326712{,}54 \cdot 10\,\% = 32671$ тенге.

Таким образом, отчисления на социальный налог составляют:
$С_н = (326712{,}54 - 32671) \cdot 11\,\% = 294042 \cdot 11\,\% = 32345$ тенге

4.5.3 Расчет амортизационных отчислений

Амортизационные отчисления рассчитываются по формуле

$$A_i = Н_A \cdot С_{ПЕР} \cdot N / 100 \cdot 12 \cdot n, \qquad (4.7)$$

где $Н_A$ – норма амортизации;
$С_{ПЕР}$ – первоначальная стоимость оборудования;
N – количество дней на выполнение работ;
n – количество дней в рабочем месяце.

Норма амортизации $Н_A$ на компьютерную технику составляет 40 % от стоимости всего оборудования.

Таким образом, амортизационные отчисления по используемому оборудованию, в соответствии с формулой 4.7 составят:

– на ноутбук:

$$A_1 = \frac{40 \cdot 125000 \cdot 48}{100 \cdot 12 \cdot 21} = \frac{240000000}{25200} = 9523{,}8 \text{ тенге}$$

– на мышь:

$$A_2 = \frac{40 \cdot 8214 \cdot 48}{100 \cdot 12 \cdot 21} = \frac{15770880}{25200} = 625{,}83 \text{ тенге}$$

$$A_3 = \frac{40 \cdot 18000 \cdot 48}{100 \cdot 12 \cdot 21} = \frac{15770880}{25200} = 1371{,}43 \text{ тенге}$$

Сводные результаты расчета амортизационных отчислений предоставлены в таблице 4.5

Т а б л и ц а 4 . 5 – Сведения по затратам на амортизацию.

Наименование оборудования	**Количество**	**Норма амортизации,**	**Сумма амортизации,**	**Цена за единицу,**

		%	тенге	тенге
Ноутбук (Samsung i3)	1	40	9523,8	125000
Мышь Razer	1	40	625,83	8214
Принтер	1	40	1371,43	18000
Итого	**-**	**-**	**11521,06**	

4.5.4 Расчет затрат на электроэнергию

Поскольку в процессе производства используется электрооборудование, необходимо рассчитать затраты на электроэнергию. Затраты на электроэнергию для производственных нужд, включают в себя расходы электроэнергии на оборудование и дополнительные нужды (формула 4.7).

$$Э = З_{эл.+эн.+обор.} + З_{доп.нуж.}, \quad (4.8)$$

где $З_{эл.+эн.+обор.}$ – затраты на электроэнергию оборудования;
$З_{доп.нуж.}$ – затраты электроэнергии на дополнительные нужды
Расходы по электроэнергии на оборудование рассчитываются по формуле

$$З_{эл.+эн.+обор.} = W \cdot T \cdot S \cdot K_{ИСП}, \quad (4.9)$$

где W – потребляемая мощность, Вт (0,8)
T – время работы
S – тариф (1 кВт = 21 тг/кВт·ч). Без НДС.
$К_{ИСП}$ – коэффициент использования ($К_{ИСП}$=0,9).

$З_{эл.+эн.+обор.1} = 0,8 \cdot 344 \cdot 21 \cdot 0,9 = 5201$ тенге

$З_{эл.+эн.+обор.2} = 0,6 \cdot 40 \cdot 21 \cdot 0,9 = 454$ тенге

Суммарные затраты на электроэнергию основного оборудования составляют:

$З_{эл.+эн.+обор.} = 5201 + 454 = 5655$ тенге

Затраты на дополнительные нужды берутся по укрупненному показателю в размере 5 % от затрат на оборудование и составляют:

$З_{ДОП.\ НУЖ.} = 5655 \cdot 0,05 = 282,75$ тенге

Таким образом суммарные затраты на электроэнергию составляют:

$С_э = 5655 + 282,75 = 5937,75$ тенге

Сводные результаты расчета затрат на электроэнергию представлены в таблице 4.6.

Т а б л и ц а 4 . 6 – Затраты на электроэнергию

Наименование приборов	**W, Вт**	**Число рабочих дней**	**$К_{ИСП}$**	**Время работы прибора, час**	**∑W кВт/ч**	**Стоимость, тенге**
Ноутбук	0,8	48	0,9	344	323,2	5201
Принтер	0,6	5	0,9	40	16,8	454
Итого ∑W	-	-	-	-	**349**	**5655**

4.5.5 Расчет затрат на накладные расходы

Накладные расходы на разработку проекта составляют от 25 % от общей суммы затрат и рассчитываются по формуле 4.9

$$Н = ФОТ \cdot 0,25 \qquad (4.10)$$

Тогда, согласно формуле (4.9), накладные расходы будут равны:

$$Н = 0,25 \cdot 326712,54 = 81678 \text{ тенге}$$

4.5.6 Расчет стоимости по всем статьям затрат

В соответствии с произведенными расчетами по статьям затрат себестоимость проекта, согласно формуле (4.1), будет равна:

$$C = 326712,54 + 32345 + 11521,06 + 5655 + 81678 = 457912 \text{ тенге}$$

Т а б л и ц а 4 . 7 – Стоимость разработки комплекса лабораторных работ

№	Наименование статей затрат	Сумма, тенге	Структура затрат %
1	ФОТ	326712,54	57
2	Отчисления на социальные нужды	32345	5,64
3	Амортизация	11521,060	1,89
4	Затраты на электроэнергию	5655	0,603
5	Накладные расходы	81678	14,25
	Итого	457912	100

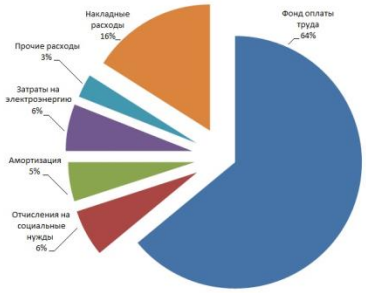

Рисунок 4.2 – Структура себестоимости комплекса лабораторных работ

4.6 Цена интеллектуального труда

Цена реализации готового продукта складывается из себестоимости и чистого дохода, и вычисляется по формуле 4.10

$$Ц = C + П \qquad (4.11)$$

где C – себестоимость продукта;
П – чистый доход.

Первоначальная цена рассчитывается через рентабельность проекта. Учитывая, что желаемый уровень рентабельности для отрасли телекоммуникации составляет 25 %, применим следующую формулу

$$Ц_{П} = C \cdot \left(1 + \frac{P}{100}\right) \qquad (4.12)$$

где P – рентабельность (25 %).

Согласно формуле 4.11 первоначальная цена равна:

$$Ц_{П} = 457912 \cdot \left(1 + \frac{25}{100}\right) = 572390 \text{ тенге}$$

Цена реализации готовой продукции рассчитывается по формуле

$$Ц_{Р} = Ц_{П} + НДС \qquad (4.13)$$

Поскольку на сегодняшний день размер НДС в РК составляет 12 %, следовательно

$$НДС = \frac{12}{100} \cdot Ц_{П} \qquad (4.14)$$

НДС = $\frac{12}{100} \cdot 572390 = 68687$ тенге

Тогда согласно формуле (4.12) цена реализации составит:

$Ц_{р}$ = 572390 + 68687= 641077 тенге

Выводы по разделу «Технико – экономическое обоснование проекта»

Дипломный проект по теме «*Разработка комплекса лабораторных работ по дисциплине «Компьютерные сети»*» имеет научно – исследовательский характер и представляет собой в основном интеллектуальный труд.

Разработка данного лабораторного комплекса является очень актуальной на сегодняшний день, так как разрабатываемые работы основаны на программе создания прототипов сети Packet Tracer компании Cisco, которая является лидирующей организацией по производству сетевого оборудования.

Цена реализации готовой продукции составила 641077 тенге.

5 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

5.1 Анализ условий труда

Рабочее помещение

Размеры рабочей аудитории: высота помещения – 3,5 м, ширина – 4 м, длина – 6 м. Общая площадь помещения составляет 24 м^2.

По разряду зрительной работы помещение относится к IV разряду с наименьшим размером объекта различения от 1 до 10 мм.

Искусственное освещение помещения состоит из люминесцентных ламп ЛБ 65-4; остекление помещения – 2 окна размером 1500×2000 мм и 2000×2000 мм.

План рабочего помещения представлен на рисунке 5.1.

Рисунок 5.1 – План помещения.

Общая площадь помещения 24 м^2. Объем рабочего помещения равняется 84 м^3, что обеспечивает необходимый объем на троих человек. Рассматривается рабочее помещения, расположенное в здании, которое не находится в непосредственной близости от железнодорожной магистрали или нагруженной автомагистрали, аэропорта и так далее, поэтому внешних источников шума, влияющих на процесс работы нет.

5.2 Оборудование и эргономические проблемы

Основным инструментарием разработки данного проекта являются ПК, которые, как и любое другое техническое оборудование, требует соблюдение техники безопасности при работе, незнание которых может привести к различным видам заболевании.

Основными недугами при длительной и неправильной работе с ПК являются головные боли, ухудшение или потеря зрения, ухудшение осанки, сколиоз, тремор, кожные воспаления и другие заболевания, резь в глазах, тянущие боли в мышцах шеи, рук и спины, зуд кожи на лице и т.д.

Основным источником эргономических проблем, связанных с охраной здоровья людей, использующих в своей работе автоматизированные информационные системы на основе персональных компьютеров, являются дисплеи (мониторы). Они представляют собой источники наиболее вредных излучений, неблагоприятно влияющих на здоровье операторов.

Частотный спектр излучения монитора характеризуется наличием рентгеновских, ультрафиолетовых, инфракрасных и других электромагнитных колебаний. Опасность рентгеновского и части других излучений большинством ученых признается пренебрежимо малой, поскольку их уровень достаточно невелик и в основном поглощается покрытием экрана. Технические характеристики дисплеев (разрешающая способность, яркость, контрастность, частота кадровой развертки) в том случае, если на них не обращают внимания при выборе устройства или неправильно устанавливают, могут крайне отрицательно сказаться на зрении.

Другой опасностью для здоровья является неправильная организация рабочего места: неудобная или неподходящая по размерам мебель, неудобное взаимные расположение компонентов системы персонального компьютера или отсутствие достаточного для свободных движений и смены позы места.

Также возможны кожные заболевания лица, причиной которых являются частицы взвешенной в воздухе пыли, притянутой к наэлектризованному монитору компьютера, так что вблизи него “качество” воздуха ухудшается и оператор вынужден работать в более запыленной атмосфере.

По причине выше изложенного можно придти к выводу, что правильная организация рабочего места играет важную роль в безопасности жизнедеятельности на предприятии и охране здоровья работников, которая достигается за счет строгого контроля условий труда на рабочем месте.

5.3 Анализ микроклимата

В таблице 5.1 приведены оптимальные нормы параметров микроклимата с учетом периода года согласно ГОСТ 12.0.003-88. Оборудование, установленное в рабочем помещении, не является источником выделения тепла (очень незначительное выделение тепла аппаратурой никаким образом не оказывает влияние на микроклимат рабочего помещения).

В соответствии с СанПиНом здание относится к I степени огнестойкости (здания с несущими и ограждающими конструкциями из естественных или искусственных материалов, бетона или железобетона с применением листовых негорючих материалов). Рабочее помещение по вопросам пожарной безопасности относится к классу «Д». В соответствии с типовыми правилами пожарной безопасности административные здания и отдельные помещения, и технологические установки обеспечиваются первичными средствами пожаротушения согласно нормативам.

Климатические условия эксплуатации оборудования полностью совпадают с климатическими условиями, нормируемыми для рабочего персонала.

Для вентиляции офисного помещения используются каналы естественной вентиляции, прокладываемые при строительстве здания и открытые окна летом. В теплый период года при достижении температуры в офисе свыше норм, приведенных в таблице 5.1, для поддержания оптимального микроклимата используется кондиционер. Нормальный микроклимат в офисе обеспечивает хорошее самочувствие сотрудников в любое время года, и соответственно продуктивность работы увеличивается. Таким образом, для поддержания условий микроклимата в помещении, целесообразно оборудовать его системой кондиционирования. Ниже будет приведен выбор кондиционера для офиса.

Т а б л и ц а 5.1 – Оптимальные нормы микроклимата для помещений с ПК

Период года	Категория работ	Температура воздуха °С не более	Относительная влажность воздуха, %	Скорость движения воздуха м/с
Теплый	Лёгкая – 1а Лёгкая – 1б	23-25 22-24	40-60 40-60	0,1 0,2

Естественное освещение не обеспечивает в течение всего рабочего времени необходимого освещения, так как может измениться погода, либо работы могут быть в позднее время, когда уже темнеет и естественного освещения может быть не достаточно, поэтому в рабочем помещении предусмотрена система искусственного общего освещения, состоящая из

светильников с люминесцентными лампами. Нормативы на источники света приведены в таблице 5.2.

Необходимо определить – обеспечивают ли используемые светильники и их количество освещение, соответствующее нормативам, при использовании только местного, а не комбинированного освещения.

Т а б л и ц а 5.2 – Рекомендуемые источники света при системе общего освещения

Характеристика зрительной работы по требованию к цветоразличию	Освещенность, лк	Диапазон цветов температуры источника света T_C, ^0K	Применяемый тип источника света
Различие цветных объектов при невысоких требованиях к цветоразличию	300, 400	3500-5500	ЛБ, НЛВД+МТЛ

Освещённость, необходимая для нормального выполнения работ в данном помещении: 400 лк.

Определение расчетной высоты подвеса

$$h_{расч} = H - (h_{пов} + h_{свес}) \quad (5.1)$$

$h_{РАСЧ}$ = 3-(0,8+0,1) = 2,1 м.

Найдем расстояние между светильниками

$$L_A = \lambda \cdot h_p \quad (5.2)$$

$L_A = 0{,}916 \cdot 2{,}15 = 1{,}969\ м$;

$L_B = \lambda \cdot h_p = 0{,}217 \cdot 2{,}15 = 2{,}616\ м$;

$1_A = (0{,}4 \div 0{,}5) \cdot L_A = 0{,}5 \cdot 2{,}15 = 1{,}075\ м$;

$1_B = (0{,}4 \div 0{,}5) \cdot L_B = 0{,}5 \cdot 2{,}15 = 1{,}075\ м$.

Для определения количества светильников определим световой поток, падающий на поверхность по формуле

$$F = \frac{E \cdot K \cdot S \cdot Z}{\eta} \quad , \quad (5.3)$$

где F – рассчитываемый световой поток;
E – нормированная минимальная мощность (E = 300 лк);
S – площадь, освещаемого помещения (S = 120 м^2);
Z – отношение средней освещенности к минимальной (Z = 1,1);
K – коэффициент запаса (K = 1,2);
η – коэффициент использования, зависит от характеристик светильника, размеров помещения, значения коэффициентов $P_с$, $P_п$ ($P_с$ = 30 %, $P_п$ = 50 %). Значение η определим по таблице коэффициентов использования светового потока. Для этого вычислим индекс помещения

$$i = \frac{S}{h_p \cdot (a+b)} \qquad (5.4)$$

$$i = \frac{12 \cdot 10}{2{,}1 \cdot (12+10)} = 2{,}6.$$

Зная индекс помещения, определим коэффициент использования светового потока: $\eta = 45\,\%$.

Подставим все значения в формулу (5.1) для определения светового потока F:

$$F = \frac{300 \cdot 1{,}2 \cdot 120 \cdot 1{,}1}{0{,}45} = 105600 \text{ лм.}$$

Для освещения выбираем люминесцентные лампы типа ЛБ40-2, световой поток которых F = 4400 Лм.

Рассчитаем необходимое количество ламп по формуле

$$N = \frac{F}{F_Л} \qquad (5.5)$$

где N – определяемое количество ламп;
F – световой поток (F = 105600 лм);
$F_Л$ – световой поток лампы ($F_Л$ = 4400 лм).

$$N = \frac{105600}{4400} = 24 \text{ шт.}$$

Для обеспечения необходимой освещенности помещения с параметрами 12×10×3 необходимо установить количество светильников типа ЛБ40-4 до 24 штук.

5.4 Рациональная организация рабочего места оператора

В связи с тем, что работа производится оператором постоянно в положении «сидя», неправильное расположение оборудования и его неудобное положение на рабочем месте могут привести к нежелательным физиологическим изменениям, повышенной утомляемости, и, как следствие, повышению производственного травматизма.

Поэтому расположение технических средств и кресла оператора в рабочей зоне должно обеспечивать:

- удобный доступ к основным функциональным узлам и блокам аппаратуры;
- исключение случайного приведения в действие средств управления и ввода информации;
- удобную рабочую позу и позу отдыха;

Наиболее оптимальное размещение оборудования оператора представлено на рисунке 5.2.

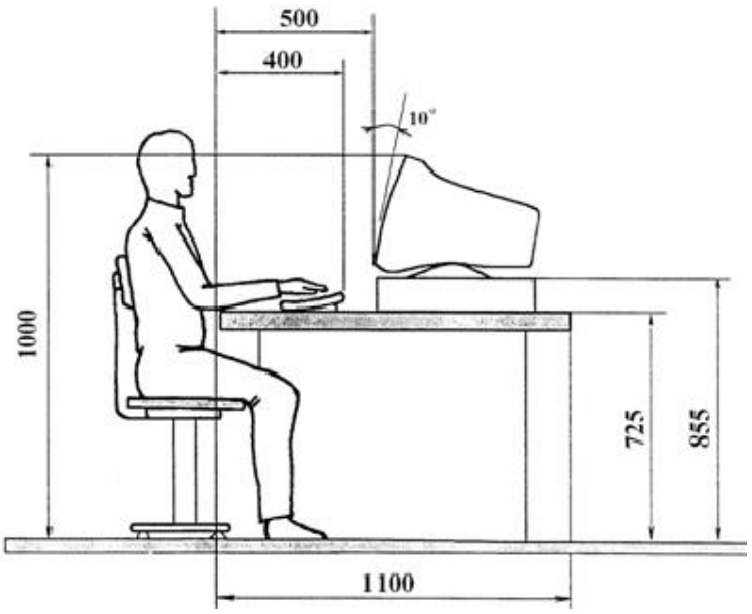

Рисунок 5.3 - Оптимальные характеристики рабочего места оператора

Одним из главных средств отображения информации и одной из основных составных частей ПК является дисплей. Именно с него оператор-студент получает данные о состоянии объекта управления и результаты

своей деятельности. Для хорошего восприятия информации, включающего соответствующую читаемость, скорость и точность считывания, зрительная индикация должна удовлетворять определенным эргономическим требованиям.

Дисплей размещается на столе или подставке так, чтобы расстояние наблюдения информации на экране не превышало 700 мм от глаз пользователя.

Для букв и цифр рекомендуются значения от 15 до 18 мм. Экран дисплея по высоте располагается так, чтобы угол между нормалью к центру экрана и горизонтальной линией взгляда составлял 20 °С. В горизонтальной плоскости угол наблюдения экрана не должен превышать 60 °С.

Клавиатура размещается на столе или подставке так, чтобы высота клавиатуры по отношению к полу составляла 650-720 мм, для того чтобы положение рук оператора было параллельно поверхности стола, а кисти были расположены над столом на высоте не более 20-35 мм при работе на клавиатуре. Это положение позволяет расслабляться рукам в перерывах между печатанием и не напрягает кисти и предплечья.

Для ввода оператором данных документ рекомендуется располагать на расстоянии 500 мм от глаза оператора, преимущественно слева, при этом угол между экраном дисплея и документом в горизонтальной плоскости должен составлять 30-40 °С. Угол наклона клавиатуры рекомендуется устанавливать 15 °С. Экран дисплея, документы и клавиатуру необходимо расположить так, чтобы перепад яркостей поверхностей, зависящий от их расположения относительно источника света, не превышал 1:10.

При планировке рабочего места необходимо учитывать удобство расположения дисплея, клавиатуры, а также зоны досягаемости рук оператора.

5.5 Расчёт естественного освещения

Рассчитаем площадь боковых световых проёмов в помещение, необходимую для создания нормируемой освещённости на рабочем месте.

Помещение имеет размеры: длина a = 6м, ширина b = 4м, высота h = 3,5м. Высота рабочей поверхности над уровнем пола – 0,7 м, окно начинается с высоты 0,8 м, высота окна 2 м. Рабочее помещение находится в IV часовом поясе – город Алматы. Со всех сторон затеняющих зданий нет.

Рабочее место расположено в 0,5 м от наружной стены помещения, где проектируем оконные проёмы. Общую требуемую площадь окон S_0, м² определим по формулам:

$$100 \cdot \frac{S_0}{S_n} = \frac{e_n \cdot \eta_0}{\tau_0 \cdot r_1} \cdot k_{зд} \cdot k_з \ , \qquad (5.6)$$

$$S_0 = \frac{S_n \cdot e_n \cdot \eta_0 \cdot k_{зд} \cdot k_з}{100 \cdot \tau_0 \cdot r_1} \quad , \qquad (5.7)$$

где S_n – площадь помещения, м²;

e_n – нормированное значение КЕО;

$k_з$ – коэффициент запаса. $k_з$ = 1,2 (учебные помещения, лаборатории, конструкторские бюро);

$k_{зд}$ – коэффициент, учитывающий затенение окон противостоящими зданиями. Поскольку затеняющих зданий поблизости нет, то $k_{зд}$ = 1;

τ_0 – общий коэффициент светопропускания;

η_0 - световая характеристика окон.

Площадь помещения равна

$$S_n = a \cdot b = 6 \cdot 4 = 24 \text{ м}^2$$

Определим нормированное значение КЕО для IV разряда зрительных работ по формуле:

$$e_n^{IV} = e_n \cdot m \cdot c \quad , \qquad (5.8)$$

где m = 0,9;

c = 0,75 – для IV часового пояса (таблица 5.3).

Определим с для IV часового пояса по таблице 5.3.

Т а б л и ц а 5.3 – Значения коэффициентов m, c

Климат светового пояса	*c* при световых проёмах				
IV 50° северной широты и Южнее (Алматы и Караганда)	m	В наружных стенах зданий	в прямоугольных и трапециевидных фонарях	в фонарях типа шед.	При зенитных фонарях
	0.9	0.8	0.9	1.0	0.9
	0.9	0.75	0.85	0.95	0.85

e_n = 1,2 для работ средней точности IV подразряда.

$$e_n^{IV} = 1,2 \cdot 0,9 \cdot 0,75 = 0,81$$

τ_0 рассчитывается по формуле:

$$\tau_0 = \tau_1 \cdot \tau_2 \cdot \tau_3 \cdot \tau_4 \quad (5.9)$$

В качестве светопропускающего материала используем:

- стекло оконное листовое, двойное: $\tau_1 = 0,8$;
- вид переплёта – двойной раздельный: $\tau_2 = 0,6$;
- вид несущей конструкции – железобетонные фермы: $\tau_3 = 0,8$;
- солнцезащитные устройства – жалюзи: $\tau_4 = 1$.

Общий коэффициент светопропускания равен

$$\tau_0 = 0,8 \cdot 0,6 \cdot 0,8 \cdot 1 = 0,384$$

Отношение длины комнаты к глубине наиболее удалённой точки от окна равно $\frac{6}{3} = 2$. Отношение ширины помещения к высоте от уровня рабочей поверхности до верха окна равно $\frac{4}{2,1} = 1.9$. Отсюда $\eta_0 = 9,2$

Вычислим общую площадь окон:

$$S_0 = \frac{24 \cdot 0,81 \cdot 9,2 \cdot 1 \cdot 1,2}{100 \cdot 0,384 \cdot 1} = 5,6 \text{ м}^2$$

Так как в кабинете общая площадь окон составляет 7 м^2, следовательно они соответствуют нормативам естественного освещения рабочего помещения.

5.6 Расчёт искусственного освещения методом коэффициента использования

Расчет искусственного освещения в помещениях можно производить следующими четырьмя методами: точечным, ватт (по таблицам удельной мощности), графическим и методом коэффициента использования.

Произведём расчеты с помощью метода коэффициента использования:

Разряд зрительной работы – IV. Нормируемая освёщенность по таблице 4.4 – 400 лк.

Т а б л и ц а 5.4 – Технические характеристики газоразрядных лампы ЛБ

Номинальная мощность, Вт	Номинальный световой поток ламп типа ЛБ, лм	Размеры ламп, мм	
65	4600	Диаметр	Длина по штырькам
		40	1514,2

В качестве светильника возьмем ЛСП24-65-101. Длина светильника 1590 мм, ширина 190 мм.

Расчёт искусственного освещения производим методом коэффициента использования.

Коэффициенты отражения от потолка стен и пола соответственно равны $\rho_{пот} = 70\ \%, \rho_{ст} = 50\ \%, \rho_{пол} = 30\ \%$.

Вычислим высоту подвеса светильника над рабочей поверхностью по формуле:

$$H = \mathrm{h} - h_p - h_c \quad , \quad (5.10)$$

где h_C – расстояние от светильника до перекрытия, h_C = 0,05 м;
h_p – высота рабочей поверхности над полом, h_p = 0,7 м;
h – высота помещения, h = 3,5 м.

$$H = 3{,}5 - 0{,}05 - 0{,}7 = 2{,}75\ \text{м}$$

Наилучшее расстояние от окна до светильника определяется по формуле:

$$\mathrm{L} = \lambda \cdot \mathrm{H} \quad , \quad (5.11)$$

где $\lambda = 1{,}2 \div 1{,}4$,

$$L = 1{,}25 \cdot 2{,}75 = 3{,}44\ \text{м}$$

Расстояние от стены до ближайшего светильника, когда работа у стены не проводится, определяем по формуле:

$$l_1 = (0{,}4 \div 0{,}5) \cdot L \quad (5.12)$$

$$l_1 = 0{,}4 \cdot 3{,}44 = 1{,}375\ \text{м}$$

Определяем индекс помещения по формуле:

$$i = \frac{l \cdot s}{H \cdot (l + s)} \quad (5.13)$$

$$i = \frac{4 \cdot 2}{2{,}75 \cdot (4 + 2)} = 0{,}48$$

Коэффициент использования в данном случае равен $\eta = 65\%$, коэффициент запаса равен $k_Z = 1{,}2$.

Определим количество люминесцентных ламп по формуле:

$$N = \frac{E \cdot k_Z \cdot S_{OC} \cdot Z}{n \cdot \Phi_Л \cdot \eta} \quad (5.14)$$

где $S_{ОС}$ – площадь помещения;

k_Z – коэффициент запаса;

E – заданная минимальная освещённость, E = 400 лк;

Z – коэффициент неравномерности освещения, Z = 1,1;

n – количество ламп в светильнике;

$\Phi_л$ – световой поток выбранной лампы, Фл = 4600 лм;

η – коэффициент использования, η = 65%.

$$N = \frac{400 \cdot 1{,}2 \cdot 24 \cdot 1{,}1}{1 \cdot 4600 \cdot 0{,}65} \approx 4$$

Всего для создания нормируемой освещенности 400 лк необходимо 4 люминесцентных ламп серии ЛД, мощность каждой лампы должна быть не меньше 65 Вт, что соответствует действительности, а значит имеющегося в наличии освещения достаточно для соответствия санитарным нормам.

5.7. Расчет системы кондиционирования

Определим необходимое количество кондиционеров для создания комфортных условий труда в помещении. В помещении за счёт тепловыделений производственного оборудования могут иметь место значительные избытки тепла (разность между тепловыделениями в помещении и теплоотдачей через стены, окна, двери и т.д.), удаление которых, прежде всего, должна обеспечить система вентиляции.

Избыточное тепло определяется по формуле:

$$Q_{ИЗБ} = Q_{ОБ} + Q_{ОСВ} + Q_Л + Q_Р - Q_{ОТД} \quad (5.15)$$

где $Q_{ОБ}$, $Q_{ОСВ}$, $Q_Л$ – тепло, выделяемое производственным оборудованием, системой искусственного освещения помещения и работающим персоналом (людьми) соответственно, ккал/ч;

$Q_Р$ – тепло, вносимое в помещение солнцем (солнечная радиация), ккал/ч;

$Q_{ОТД}$ – теплоотдача естественным путём, ккал/ч.

Тепло, выделяемое производственным оборудованием определяется по формуле:

$$Q_{ОБ} = 860 \cdot P_{ОБ} \cdot \eta \quad , \quad (5.16)$$

где 860 – тепловой эквивалент 1 кВт/ч;

РОБ – мощность, потребляемая оборудованием, кВт/ч;

η – коэффициент перехода тепла в помещение.Значение η = 0,95 – норма потерь потребляемой мощности на тепловыделения компьютерного оборудования.

Для 1 компьютера имеем:

$$Q_{ОБ} = 860 \cdot (1 \cdot 0{,}25) \cdot 0{,}95 = 204{,}25 \text{ ккал/ч}$$

Тепло, выделяемое осветительными установками, рассчитывается по формуле:

$$Q_{ОСВ} = 860 \cdot N \cdot \eta \quad , \quad (5.17)$$

где N – расходуемая мощность светильников, кВт;

η = 0,55 – норма потерь потребляемой мощности на тепловыделения люминесцентных ламп.

$$Q_{ОСВ} = 860 \cdot 0{,}55 \cdot 0{,}52 = 246 \text{ ккал/ч}$$

Тепло, выделяемое людьми, рассчитывается по формуле:

$$Q_Л = К_Л \cdot (q - q_{ИСП}) \quad , \quad (5.18)$$

где $К_Л$ – количество работающих;

$(q - q_{ИСП})$ – явное тепло, ккал/ч;

q – тепловыделения одного человека при данной категории работ I-III, ккал/ч.

Работа, производимая в помещении, относится к I категории работ: q = 100 Вт, или 0,1 кВт для офисных помещений.

$$Q_Л = 1 \cdot 860 \cdot 0{,}1 = 86 \text{ ккал/ч}$$

Тепло, вносимое солнечной радиацией, рассчитывается по формуле:

$$Q_Р = m \cdot F \cdot q_{ОСТ} \quad (5.19)$$

где m – количество окон в помещении;
F – площадь одного окна, м^2;
$q_{ост}$ – солнечная радиация через остеклённую поверхность, т.е. количество тепла, вносимое за один час через остеклённую поверхность площадью 1 м^2.

Для окна с двойным остеклением с деревянными переплетами $q_{ост}$ = 105 (окна выходят на север, Алматы находится на широте 43° сев. широты). Количество окон равно 2. Площадь окна равна $2 \cdot 1{,}5 = 3 м^2$.

$$Q_Р = 1 \cdot 3 \cdot 105 = 315 \text{ ккал/ч}$$

Для тёплого периода года при расчётах можно принять $Q_{ОТД}$ = 0.

$$Q_{ИЗБ} = 204{,}25 + 246 + 85 + 315 = 851{,}3 \text{ ккал/ч}$$

При наличии теплоизбытков количество воздуха, которое необходимо удалить из помещения рассчитывается по формуле:

$$L_b = \frac{Q_{ИЗБ}}{C_b \cdot \Delta t \cdot \gamma_b} \quad (5.20)$$

где $Q_{ИЗБ}$ – избыточное тепло, ккал/ч;
C_b – теплоёмкость воздуха (0,24 ккал/кг °С);
$\Delta t = t_{вых} - t_{вх}$;

$t_{вых}$ – температура воздуха выходящего из помещения, °С;
$t_{вх}$ – температура воздуха поступающего в помещение, °С;

γ_b = 1,206 кг/м^3 – удельная масса приточного воздуха.

Величина Δt при расчётах выбирается в зависимости от теплонапряжённости воздуха и рассчитываются по формуле 5.21

$$Q_н = \frac{Q_{изб}}{V_п} \quad (5.21)$$

$$Q_н = \frac{851,3}{96} = 887 \text{ ккал/м}$$

Если теплонапряжённость воздуха $Q_н$<20 ккал/м^3, то принимают $\Delta t = 6℃$, а при $Q_н$>20 ккал/м^3, $\Delta t = 8℃$.

$$L_b = \frac{851,3}{0,24 \cdot 8 \cdot 1,206} = 367,6 \, м^3/ч$$

Существующий оконный кондиционер имеет расход воздуха 450 м3/ч. Определим требуемое количество таких кондиционеров:

$$N = \frac{367,6}{450} \approx 1 \, кондиционер$$

Что соответствует действительности и является достаточным для обеспечения комфортного микроклимата.

ЗАКЛЮЧЕНИЕ

В разделе «Безопасность жизнедеятельности» были изложены требования к рабочему месту пользователя. Созданные условия должны обеспечивать комфортную работу. На основании изученной литературы по данной проблеме, также проведен выбор системы и расчет оптимального освещения производственного помещения, устаревшей компьютерной техники. Соблюдение условий, определяющих оптимальную организацию рабочего места, позволит сохранить хорошую работоспособность в течение всего рабочего дня, повысит как в количественном, так и в качественном отношениях производительность труда программиста, что в свою очередь будет способствовать быстрейшему выполнению и отладке лабораторных работ.

ЗАКЛЮЧЕНИЕ

В дипломном проекте предложен комплекс лабораторных работ, направленный на изучение компьютерных сетей и систем.

Комплекс работ оформлен в виде методических указаний к выполнению лабораторных работ и включает в себя теоретическую и практическую части. В теоретической части приведены основные теоретические выкладки и описание системы команд, необходимых для использования в лабораторной работе. Практическая часть представляет собой пошаговую инструкцию к выполнению лабораторной работы.

Результатом внедрения предлагаемого комплекса является:

- углубленное изучение вопросов безопасности сетей;
- повышение качества знаний и уровня квалификации студентов;
- повышение престижа ВУЗа.

СПИСОК ЛИТЕРАТУРЫ

1 Сайт http://www.seti.com.ua. – Журнал *Сети и телекоммуникации. – №7–8*

2 Дьеченко В.А., Анализ проблем информационной безопасности в компьютерной сети, организации подключенной к сети Интернет. – М., 2009.

3 Сайт http://www.opennet.ru/docs/RUS/vpn_ipsec/

4 Сайт http://ru.wikipedia.org/wiki/IPsec#Security_Policy_Database

5 Николай Колдовский. Построение безопасных сетей на основе VPN. – М.: Инфра–М, 2011.

6 Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник. – Санкт–Петербург: Питер, 2001.

7 Щербо В.К. Стандарты вычислительных сетей. – М.: Кудиц–Образ, 2000.

8 Верховский Е.И. Пожарная безопасность на предприятиях радиоэлектроники. – М.: Высшая школа, 1987.

9 Аманбаев У.А. Экономика предприятия. –Алматы: Бастау, 2012.

10 Буров В.П. Бизнес–план фирмы. – М.: Инфра–М, 2011.

11 Куатова Д.Я. Экономика предприятия. – Алматы: Экономика, 2011.

12 Еркешева З.Д., Боканова Г.Ш., Методические указания к выполнению экономической части дипломных работ для студентов специальности 5В070400 – Вычислительная техника и программное обеспечение. – Алматы: АУЭС, 2014. – 40 с.

13 Сайт http://kunegin.narod.ru/ref5/ipsec/doc09.htm

14 Сайт http://www.opennet.ru/docs/RUS/vpn_ipsec/

15 Сайт http://www.ixbt.com/comm/ipsecure.shtml

16 Сайт http://daily.sec.ru/2008/09/08/Virtualnie–chastnie–seti–vibor–optimalnogo–podhoda.html

17 Сайт http://www.micom.net.ru/networks/

ПРИЛОЖЕНИЕ А

СПИСОК ОСНОВНЫХ КОМАНД ИНТЕРФЕЙСА IOS CLI

Команда	Описание	Команда	Описание
?	Выводит список доступных команд. После вывода одного экрана появляется приглашение --more--, указывающее, что на экран выведена не вся информация. Для построчного просмотра необходимо нажать *ENTER* или клавишу *ПРОБЕЛ*, для вывода следующего экрана.	antenna gain| receive| transmit	Установка параметров антенны точки доступа. Возможны следующие опции: – gain – показать усиление антенны в децибелах; – receive – настроить антенну на прием данных; – transmit – настроить антенну на передачу данных.
enable	Переход в привилегированный режим. После ввода команды необходимо ввести пароль.	copy running-config startup-config	Скопировать текущую конфигурацию на место начальной.
disable	Возврат в пользовательский режим.	shutdown	Отключение интерфейса.
exit, quit	Выход из любого режима и завершение сеанса работы с точкой доступа.	no	Для отключения функционирования или полного изменения действия команды.
show	Вывести текущую информацию о системе.	hostname *name*	Задание имени точки доступа.
configure terminal	Вход в режим конфигурации.	erase startup-config	Удаление начальной конфигурации точки доступа.
authentication open [eap]	Задание открытой аутентификации для беспроводной сети. Можно использовать также опцию eap аутентификации. Добавление этой опции позволяет использовать eap-аутентификации для клиентских адаптеров с открытой аутентификацией. Open аутентификация может использоваться для шифрования как WEP, так и WPA, WPA-PSK.	dot11 mbssid	Включение на точке доступа возможности множественного идентификатора SSID. Используется для передачи в широковещательном пакете (beacon) более одного идентификатора сети (например, если существуют несколько виртуальных сетей).
ip address *ip address mask*	Ввод IP адреса и маски подсети точки доступа.	dot11 ssid *ssid*	Глобальная настройка идентификатора SSID. Параметр *ssid* – название беспроводной сети.
ssid *ssid*	Назначение идентификатора SSID точки доступа.	interface bvi1	Настойка интерфейса BVI.
authentication key-management wpa|cckm	Задание аутентификации пользователей с использованием WPA или CCKM управлений ключами. Требует наличия открытой или открытой вместе с eap аутентификациями. Может использоваться как для WPA-шифрования, так и для WPA-PSK.	authentication shared [eap]	Установка аутентификации с общим ключом. Также есть возможность выбора и опции eap аутентификации. Данный тип аутентификации используется для WEP шифрования или для WPA-PSK.
interface dot11radio 0	Настройка радио интерфейса на 2.4 ГГц (стандарт 802.11g).	guest-mode	Назначение широковещательного режима идентификатора сети.
max-associations *number*	Установка максимального количества устройств, которые могут подключиться к точке доступа.	dot11 vlan-name *name* vlan *ID*	Назначение имени для определенной виртуальной сети

wpa-psk ascii|hex *encryption-key*	Задание ключевой WPA фразы. Для соединения с сетью на клиенте также должна быть установлена опция WPA-PSK и введена ключевая фраза (*encryption-key*).	vlan *ID*	Определение идентификатора сети SSID к виртуальной сети. Для каждой виртуальной сети может быть создан только один SSID. Точки доступа поддерживают до 16 SSID.
encryption [vlan *ID*] mode ciphers|wep	Настройка для беспроводной сети определенного типа шифрования. WPA шифрование поддерживает cipher TKIP или AES (используется при network-eap аутентификации). Для WEP шифрования выбирается тип wep mandatory (принудительное) или wep option (опциональное, настраиваемое). Возможно также совместное использование нескольких типов шифрования, например, encryption mode ciphers tkip wep40|wep128 или mode ciphers wep40|wep128 mic key-hash. При создании нескольких виртуальных сетей, для каждой из них может быть задан свой тип шифрования.	mbssid guest-mode dtim-period *seconds*	Настройка текущего идентификатора SSID как множественного (Multiple Basic SSID), т.е. включение в широковещательный пакет (beacon) текущего SSID. Это сделает беспроводную сеть более гостеприимной. Точки доступа поддерживают до 8 mbssid. Для каждого SSID можно установить свой dtim-period, как часто будет содержать пакет сообщение о индикации трафика поставки сети. Слишком маленькое значение уменьшает время жизни батарейки клиента (ноутбука), слишком маленькое значение может сделать беспроводную сеть менее гостеприимной.
power	Установка уровня мощности сигнала на точке доступа или клиенте.	bridge-group *ID*	Задание группы моста для каждой виртуальной сети (должна быть своя группа моста, равная номеру vlan).
speed	Установка скорости передачи данных.	station-role	Определение роли точки доступа в беспроводной сети.
channel	Определение канала.	server *address* auth-port 1812 acct-port 1813	Добавление сервера к существующей группе серверов.
broadcast-key [vlan *ID*] change *seconds* [membership-termination] [capability-change]	Назначение периода между вещаниями ключа. Широковещание ключа устанавливается для виртуальной сети или для всего радио интерфейса. Опция membership-termination позволяет точке доступа генерировать новые ключи при отключении любого клиентского устройства от нее и распространить их. Опция capability-change – точка доступа генерирует и широковещает новую динамическую группу ключей, когда последнее клиентское устройство с статическим WEP отключается от нее и распространяет статический WEP ключ при подключении первого клиентского устройства с статическим WEP.	encryption [vlan *ID*] key *number* size 40|128 *key* transmit-key	Задание WEP ключа на точке доступа. Для соединения с беспроводной сетью клиентское устройство также должно содержать аналогичный WEP ключ. На точке доступа может быть создано 4 WEP ключа, но использоваться только один. Номер ключа задается с помощью опции number, после этого указывается размер ключа и сам ключ. 40 битный ключ должен содержать 10 шестнадцатеричных символов, а 128 битный – 24. Опция transmit-key позволяет установить данный ключ как активный, т.е. передаваемый. По умолчанию активным (transmit-key) назначен первый ключ.
encapsulation dot1q *ID* [native]	Активация виртуальной сети для радио интерфейса. Опция native назначает данную виртуальную сеть главной.	ip dhcp excluded-address *low high*	Задание запрещенных IP адресов для DHCP сервера. Low – нижняя граница, high – верхняя граница. Может быть задана только нижняя граница – все адреса выше заданного считаются запрещенными в данной подсети.

network *subnet_number* [*mask*]	Задание подсети для DHCP сервера.	ip dhcp pool *pool_name*	Задание имени для пула адресов.
aaa new-model	Создание новой модели протокола AAA.	radius-server local	Создание локального RADIUS сервера на точке доступа.
parent *[1-4] mac address [timeout]*	Установка точки доступа-родителя, к которой подключается репитер. Можно ввести до 4 родителей: репитер вначале подключается к первой, если она не отвечает или превышен интервал ожидания (timeout), то выполняет подключение к следующей.	lease *days*|*hours*| *minutes*	Время аренды выданного адреса, Может быть задано в днях, часах или минутах.
default-router *address*	Адрес маршрутизатора по умолчанию. Необходимо для обеспечения выхода клиентов в Интернет.	infrastructure-ssid	Назначение данного идентификатора сети, который объединяет все точки доступа и мосты рабочих групп этой сети. Без установки этой опции подключение к другой точке доступа можно выполнить только используя другой SSID.
authentication open eap *name*	Открытая аутентификация с использованием метода EAP с названием name.	beacon period| dtim-period	Настройка широковещательного пакета (beacon): – period – установка временного интервала между пакетами в киломикросекундах (Один Kμsec равняется 1024 микросекундам); – dtim-period – как часто будет содержать пакет сообщение о индикации трафика поставки сети.
authentication network-eap eap *name*	Аутентификация через RADIUS сервер. Метод аутентификации с названием name.	username *name* password *key*	Создание базы пользователей на локальном RADIUS сервере. При аутентификации необходимы введенные данные со стороны клиента.
nas *address* key *key*	Указание на RADIUS сервере адреса точек доступа-аутентификаторов. При подключении к RADIUS серверу для проведения аутентификации пользователей точка доступа должна передать секретный ключ key.	radius-server host *address* auth-port *port* acct-port *port* key *key*	Указание точке доступа адрес RADIUS сервера и портов аутентификации и учета. Для локального сервера используются порты auth-port 1812 acct-port 1813. Ключ должен совпадать с ключом заданным в RADIUS сервере для данного аутентификатора.
aaa group server radius *name_group*	Создание группы серверов, к которым должна обращаться точка доступа при выполнении аутентификации.	aaa authentication login *name* group *name_group*	Указание использования на точке доступа метода name для определенной группы серверов при аутентификации пользователей.