МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Кафедра «Электроника»

«Допущен к защите»
Зав. кафедрой «Электроника»

_____

А.А. Копесбаева к.т.н., проф.
«___»_____2014г.

ДИПЛОМНЫЙ ПРОЕКТ

На тему: «Разработка локальной сети компании с расширенными функциональными возможностями»

Специальность «5В071900 – Радиотехника, электроника и телекоммуникации»

Выполнил _____ ст. гр. ЭСТ-10-1 Б.А.Канафина

Научный руководитель _____ Б.С. Байкенов к.т.н, доц.

Консультанты:
по экономической части:
Бекишева А.И., к.э.н., доцент

_____ «5» марта 2014 г.
(подпись)

по безопасности жизнедеятельности:
Санатова Т.С., к.т.н., доцент

_____ «23» мая 2014 г.
(подпись)

Нормоконтролер: Байкенов Б.С., к.т.н., доцент

_____ «26» мая 2014 г.
(подпись)

Рецензент: З.М. Ярмухамедова к.т.н, проф.

_____ «_____»_____20___г.
(подпись)

Алматы 2014 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Факультет «Радиотехники и связи»
Специальность «5В071900 – Радиотехника, электроника и телекоммуникации»
Кафедра «Электроника»

ЗАДАНИЕ
на выполнение дипломного проекта

Студента Б.А.Канафина

Тема проекта «Разработка локальной сети компании с расширенными функциональными возможностями» утверждена приказом ректора № 115 от 24 сентября 2013 г.

Срок сдачи законченной работы « 15» мая 2014г.

Исходные данные к проекту (требуемые параметры результатов проектирования) и исходные данные корпоративной сети.

Перечень подлежащих разработке в дипломном проекте вопросов или краткое содержание дипломного проекта

1. Технологическая часть (общее описание локальных сетей, сетевых технологий и протоколов).
2. Конструкторский часть (планирование сети, выбор топологии и оборудования).
3. Программная часть (листинг настройки сети командами Cisco IOS).
4. Общие вопросы охраны труда (расчет освещения и пожарной безопасности помещения).
5. Технико–экономическая часть (расчет экономического эффекта от внедрения данной технологии).

Перечень графического материала (с точным указанием обязательных чертежей): в данной работе содержится 19 рисунков и 7 таблиц.

Рекомендуемая основная литература:

1) Олифер В.Г., Олифер Н.А. Принципы, технологии, протоколы. Учебник для вузов: С.-Пб.; Энергоатомиздат. Санкт-Петербургское отд-ние, 2010.-944 с.
2) Хилл Б. Полный справочник по Cisco: Пер. с англ. – М.: ООО «И.Д. Вильямс», 2004. – 1068 с.
3) Одом У. Официальное руководство по подготовке к сертификационным экзаменам CCNA ICND2: Пер. с англ. – М.: ООО «И.Д. Вильямс», 2009. – 7[illegible] с.
4) Князевский Б.А. Охрана труда. – М.: Высшая школа, 2002. – 365 с.
5) Базылов К.Б., Алибаева С.А., Бабич А.А. Выпускная работа бакалавров. Экономический раздел. – Алматы: АИЭС, 2008. - 20 с.

Консультанты по проекту с указанием относящихся к ним разделов работы

Раздел	Консультант	Сроки	Подпись
Технологическая часть	Байкенов Б. С.	30.03.14	
Разработка сети	Байкенов Б. С.	15.04.14	
Программное обеспечение	Байкенов Б. С.	30.04.14	
Безопасность жизнедеятельности	Санатова Т.С.	4.05.14	
Экономическая часть	Бекишева А. И.	10.05.14	

ГРАФИК
подготовки дипломного проекта

№ п/п	Наименование разделов	Сроки представления	Примечание
1	2	3	4
1	1. Технологическая часть 1.1 Понятие и классификация локальных сетей 1.2 Стандартная сетевая модель OSI 1.3 Стек протоколы TCP/IP 1.4 Структурные схемы локальных сетей 1.5 Технология Fast Ethernet 1.6 Технология VPN и удаленный доступ 1.7 Технология IP-телефонии 1.8 Технология Wi-Fi	30.03.14	
2	2. Конструкторская часть 2.1 Планирование сети 2.2 Сетевое оборудование 2.3 Логическая топология сети	15.04.14	
3	3 Программное обеспечение 3.1 Среда моделирования 3.2 Листинг настройки 3.3 Защита информации на файловом сервере 3.4 Настройка доступа в Интернет 3.5 Агрегирование каналов	30.04.14	
4	4. Безопасность жизнедеятельности	5.05.14	
5	5. Бизнес-план	10.05.14	

Дата выдачи задания «19» марта 2014г.

Заведующий кафедрой А.А. Копесбаева

Руководитель Б.С. Байкенов

Задание принял к исполнению
студент Б.А. Канафина

АНДАТПА

Бұл дипломдық жоба корпоративтік Fast Ethernet желі өңдеуіне арнаулы. Технологиялық және қанаушылық сұрақтар қаралған, икемдеу Cisco IOS командаларымен жасалынған. Жобаланған жүйенің негізгі еңгізу ісі техника қауіпсіздігі есептеулері және жобаның бизнес-жоспары арқылы расталған.

АННОТАЦИЯ

Дипломный проект посвящен разработке локальной сети компании с расширенными функциональными возможностями. Рассмотрены технологические и эксплуатационные вопросы, произведена настройка командами Cisco IOS. Целесообразность внедрения разработанной системы подтверждена технико-экономическим расчетом.

SUMMORY

Thesis project is dedicated to the development of a local network with broadned functional possibilities. Examined the technological and operational issues is tuned commands Cisco IOS. The feasibility of the developed system confirmed the technical and economic calculation.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Построение локальной сети является на сегодняшний день наилучшим способом создания в компании единой информационной среды, обусловленного современными требованиями быстрого обмена информацией между пользователями, совместного использования различных ресурсов.

Локальная сеть предназначена для сбора, передачи, рассредоточенной и распределенной обработки информации в пределах одной лаборатории, отдела, офиса или компании, часто специализируется на выполнении определенных функций соответственно профилю деятельности компании и отдельных ее подразделов. Во многих случаях локальная сеть, обслуживающая свою локальную информационную систему, связанна с другими вычислительными сетями, внутренними или внешними, вплоть до региональных или глобальных сетей.

Целью данной дипломной работы является разработка корпоративной локальной сети компании с расширенными функциональными возможностями.

Эффективность разработанной локальной сети компании не вызывает сомнения, поскольку обеспечивает следующие преимущества:

- совместный непрерывный доступ к корпоративным ресурсам;
- совместное пользование дорогостоящей оргтехникой;
- возможность работать удаленно из любой точки земного шара;
- быстрое и простое перемещение и добавление новых рабочих мест и оборудования;
- обеспечение дополнительной безопасности корпоративных данных особой секретности и другие преимущества.

1 ТЕХНОЛОГИЧЕСКАЯ ЧАСТЬ

1.1 Понятие и классификация локальных сетей

Локальная сеть – это *группа из нескольких компьютеров, соединённых между собой посредством кабелей (иногда также телефонных линий или радиоканалов), используемых для передачи информации между компьютерами [14]*.

Сеть, которая организует взаимодействие в ограниченной области, называется локальной вычислительной сетью (ЛВС). Достаточно часто ЛВС размещается в одном месте (например, в офисе). Глобальная вычислительная сеть (ГВС) - это группа устройств или ЛВС, которые располагаются в разных удаленных друг от друга местах и связываются между собой телефонными каналами, высокоскоростными выделенными линиями, оптоволоконными и спутниковыми каналами. Самый известный пример ГВС - Internet.

При создании сетей наиболее часто используются технологии Ethernet и Fast Ethernet. Причем несколько технологий могут использоваться в одной сети. Ethernet-сети и Fast Ethernet-сети функционируют аналогично; главное отличие заключается в скорости передачи данных. Ethernet-сети работают со скоростью 10 Мбит в секунду (Мбит/с), а Fast Ethernet - со скоростью 100 Мбит/с и выше [14].

Чаще всего в локальных сетях используется статическая либо динамическая маршрутизация (основанная на протоколе RIP). В более крупных локальных сетях возможно и появление более сложных протоколов маршрутизации (OSPF, BGP).

Иногда в локальной сети организуются рабочие группы — формальное объединение нескольких компьютеров в группу с единым названием (VLAN).

Локальные сети классифицируются по типу функционального взаимодействия [14].

1.1.1 Технология «клиент-сервер»

Клиент-сервер (англ. Client/Server) — сетевая архитектура, в которой устройства являются либо клиентами, либо серверами. Клиентом (front end) является запрашивающая машина (обычно ПК), сервером (back end) — машина, которая отвечает на запрос. Оба термина (клиент и сервер) могут применяться как к физическим устройствам, так и к программному обеспечению [13].

Сеть с выделенным сервером (англ. Client/Server network) — это локальная вычислительная сеть (LAN), в которой сетевые устройства централизованы и управляются одним или несколькими серверами. Индивидуальные рабочие станции или клиенты (такие, как ПК) должны обращаться к ресурсам сети через сервер или серверы.

1.1.2 Сеть точка-точка

Сеть точка-точка — простейший вид компьютерной сети, при котором два компьютера соединяются между собой напрямую через коммуникационное оборудование. Достоинством такого вида соединения является простота и дешевизна, недостатком — соединить таким образом можно только 2 компьютера и не больше [14].

Часто используется, когда необходимо быстро передать информацию с одного компьютера, например, ноутбука, на другой.

Широкое распространение получила в Bluetooth сетях мобильных устройств.

1.1.3 Одноранговые сети

Одноранговые, децентрализованные или пиринговые (от англ. peer-to-peer, P2P — равный с равным) сети — это компьютерные сети, основанные на равноправии участников. В таких сетях отсутствуют выделенные серверы, а каждый узел (Peer) является как клиентом, так и сервером. В отличие от архитектуры клиент-сервер, такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов [14].

Впервые фраза «peer-to-peer» была использована в 1984 году в разработке архитектуры Advanced Peer to Peer Networking фирмы IBM.

Например, в сети есть 10 машин, при этом любая может связаться с любой. В качестве клиента (потребителя ресурсов) каждая из этих машин может посылать запросы на предоставление каких-либо ресурсов другим машинам в пределах этой сети и получать их. Как сервер, каждая машина должна обрабатывать запросы от других машин в сети, отсылать то, что было запрошено, а также выполнять некоторые вспомогательные и административные функции.

Любой член данной сети не гарантирует никому своего присутствия на постоянной основе. Он может появляться и исчезать в любой момент времени. Но при достижении определённого критического размера сети наступает такой момент, что в сети одновременно существует множество серверов с одинаковыми функциями.

В последние годы одноранговые сети используются для анонимизации пользователей в таких сетях TOR и I2P [13].

1.1.4 Частично децентрализованные (гибридные) сети

Помимо чистых P2P-сетей, существуют так называемые гибридные сети, в которых существуют сервера, используемые для координации работы, поиска или предоставления информации о существующих машинах сети и их статусе (on-line, off-line и т.д.). Гибридные сети сочетают скорость централизованных сетей и надёжность децентрализованных благодаря гибридным схемам с независимыми индексационными серверами, синхронизирующими информацию между собой. При выходе из строя одного или нескольких серверов, сеть продолжает функционировать. К частично децентрализованным файлообменным сетям относятся например EDonkey, BitTorrent [14].

1.2 Стандартная сетевая модель OSI

Сетевая модель OSI (open systems interconnection basic reference model) — сетевая модель стека сетевых протоколов OSI/ISO [13].

Модель содержит семь отдельных уровней:

- уровень 1: физический – битовые протоколы передачи информации;
- уровень 2: канальный – формирование кадров, управление доступом к среде;
- уровень 3: сетевой – маршрутизация, управление потоками данных;
- уровень 4: транспортный – обеспечение взаимодействия удаленных процессов;
- уровень 5: сеансовый – поддержка диалога между удаленными процессами;
- уровень 6: представительский – интерпретация передаваемых данных;
- уровень 7: прикладной – пользовательское управление данными.

В модели OSI сетевые функции распределены между семью уровнями. На каждом уровне выполняются определенные сетевые функции, которые взаимодействуют с функциями соседних уровней, вышележащего и нижележащего. Каждый уровень предоставляет несколько услуг (то есть выполняет несколько операций), подготавливающих данные для доставки по сети на другой компьютер. Уровни отделяются друг от друга границами — интерфейсами. Все запросы от одного уровня к другому передаются через интерфейс. Каждый уровень использует услуги нижележащего уровня. Далее описывается каждый из семи уровней модели OSI и определяются услуги, которые они предоставляют смежным уровням.

Уровень 7, Прикладной (Application), — самый верхний уровень модели OSI. Он представляет собой окно для доступа прикладных процессов к сетевым услугам. Этот уровень обеспечивает услуги, напрямую поддерживающие приложения пользователя, такие, как программное обеспечение для передачи файлов, доступа к базам данных и электронная почта. Нижележащие уровни поддерживают задачи, выполняемые на Прикладном уровне. Прикладной уровень управляет общим доступом к сети, потоком данных и обработкой ошибок.

Уровень 6, Представительский (Presentation), определяет формат, используемый для обмена данными между сетевыми компьютерами. Этот уровень можно назвать переводчиком. На компьютере-отправителе данные, поступившие от Прикладного уровня, на этом уровне переводятся в общепонятный промежуточный формат. Представительский уровень, кроме того, управляет сжатием данных для уменьшения передаваемых битов.На этом уровне работает утилита, называемая редиректором (redirector). Ее назначение — переадресовать операции ввода/вывода к ресурсам сервера.

Уровень 5, Сеансовый (Session), позволяет двум приложениям на разных компьютерах устанавливать, использовать и завершать соединение, называемое сеансом. На этом уровне выполняются такие функции, как распознавание имен и защита, необходимые для связи двух приложений в

сети. Сеансовый уровень обеспечивает синхронизацию между пользовательскими задачами посредством расстановки в потоке данных контрольных точек (chekpoints).

Уровень 4, Транспортный (Transport), обеспечивает дополнительный уровень соединения — ниже Сеансового уровня. Транспортный уровень гарантирует доставку пакетов без ошибок, в той же последовательности, без потерь и дублирования. На этом уровне сообщения переупаковываются: длинные разбиваются на несколько пакетов, а короткие объединяются в один. Это увеличивает эффективность передачи пакетов по сети. На Транспортном уровне компьютера-получателя сообщения распаковываются, восстанавливаются в первоначальном виде, и обычно посылается сигнал подтверждения приема. Транспортный уровень управляет потоком, проверяет ошибки и участвует в решении проблем, связанных с отправкой и получением пакетов.

Уровень 3, Сетевой (Network), отвечает за адресацию сообщений и перевод логических адресов и имен в физические адреса. Одним словом, исходя из конкретных сетевых условий, приоритета услуги и других факторов здесь определяется маршрут от компьютера-отправителя к компьютеру-получателю. На этом уровне решаются также такие задачи и проблемы, связанные с сетевым трафиком, как коммутация пакетов, маршрутизация и перегрузки. Если сетевой адаптер маршрутизатора не может передавать большие блоки данных, посланные компьютером-отправителем, на Сетевом уровне эти блоки разбиваются на меньшие. А Сетевой уровень компьютера-получателя собирает эти данные в исходное состояние.

Уровень 2, Канальный, осуществляет передачу кадров (frames) данных от Сетевого уровня к Физическому. Кадры — это логически организованная структура, в которую можно помещать данные. Канальный уровень компьютера-получателя упаковывает «сырой» поток битов, поступающих от Физического уровня, в кадры данных. Обычно, когда Канальный уровень посылает кадр, он ожидает со стороны получателя подтверждения приема.

Канальный уровень получателя проверяет наличие возможных ошибок передачи. Кадры, поврежденные при передаче, или кадры, получение которых не подтверждено, посылаются вторично.

Уровень 1, Физический, — самый нижний в модели OSI. Этот уровень осуществляет передачу неструктурированного, «сырого» потока битов по физической среде (например, по сетевому кабелю). Здесь реализуются электрический, оптический, механический и функциональный интерфейсы с кабелем. Физический уровень также формирует сигналы, которые переносят данные, поступившие от всех вышележащих уровней. На этом уровне определяется способ соединения сетевого кабеля с платой сетевого адаптера, в частности, количество контактов в разъемах и их функции. Кроме того, здесь определяется способ передачи данных по сетевому кабелю. Физический (Physical) уровень предназначен для передачи битов (нулей и единиц) от одного компьютера к другому. Содержание самих битов на данном уровне значения не имеет. Этот уровень отвечает за кодирование данных и синхронизацию битов, гарантируя, что переданная единица будет воспринята именно как единица, а не как ноль. Наконец, Физический уровень устанавливает длительность каждого бита и способ перевода бита в соответствующие электрические или оптические импульсы, передаваемые по сетевому кабелю[13].

1.3 Стек протоколы TCP/IP

Стек протоколов TCP/IP — набор сетевых протоколов передачи данных, используемых в сетях, включая сеть интернет. Название TCP/IP происходит из двух наиболее важных протоколов семейства — Transmission Control Protocol (TCP) и Internet Protocol (IP), которые были разработаны и описаны первыми в данном стандарте. Так как стек TCP/IP был разработан до появления модели

взаимодействия открытых систем ISO/OSI, то, хотя он также имеет многоуровневую структуру, соответствие уровней стека TCP/IP уровням модели OSI достаточно условно.

Протоколы работают друг с другом в стеке (англ. *stack*, стопка) — это означает, что протокол, располагающийся на уровне выше, работает «поверх» нижнего, используя механизмы инкапсуляции. Например, протокол TCP работает поверх протокола IP [13].

Структура протоколов TCP/IP приведена на рисунке 1.1.

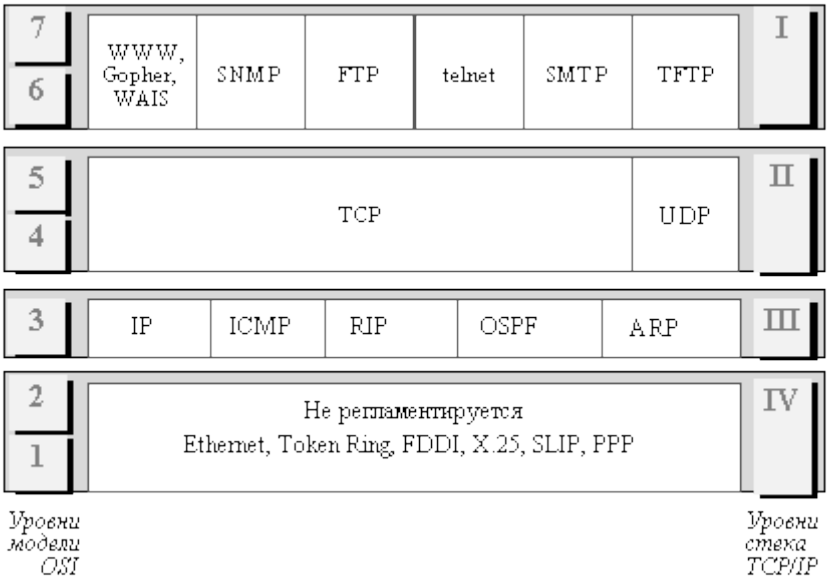


Рисунок 1.1 – Стек TCP/IP

Протоколы TCP/IP делятся на четыре уровня:

- канальный уровень (link layer);
- сетевой уровень (internet layer);
- транспортный уровень (transport layer);
- прикладной уровень (application layer).

Самый нижний (уровень IV) соответствует физическому и канальному уровням модели OSI. Этот уровень в протоколах TCP/IP не регламентируется, но поддерживает все популярные стандарты физического и канального уровня: для локальных сетей это Ethernet, Token Ring, FDDI, Fast Ethernet, 100VG-AnyLAN, для глобальных сетей - протоколы соединений "точка-точка" SLIP и

PPP, протоколы территориальных сетей с коммутацией пакетов X.25, frame relay. Разработана также специальная спецификация, определяющая использование технологии ATM в качестве транспорта канального уровня. Обычно при появлении новой технологии локальных или глобальных сетей она быстро включается в стек TCP/IP за счет разработки соответствующего RFC, определяющего метод инкапсуляции пакетов IP в ее кадры.

Следующий уровень (уровень III) - это уровень межсетевого взаимодействия, который занимается передачей пакетов с использованием различных транспортных технологий локальных сетей, территориальных сетей, линий специальной связи и т. п.

В качестве основного протокола сетевого уровня (в терминах модели OSI) в стеке используется протоколIP, который изначально проектировался как протокол передачи пакетов в составных сетях, состоящих из большого количества локальных сетей, объединенных как локальными, так и глобальными связями. Поэтому протокол IP хорошо работает в сетях со сложной топологией, рационально используя наличие в них подсистем и экономно расходуя пропускную способность низкоскоростных линий связи. Протокол IP является дейтаграммным протоколом, то есть он не гарантирует доставку пакетов до узла назначения, но старается это сделать.

К уровню межсетевого взаимодействия относятся и все протоколы, связанные с составлением и модификацией таблиц маршрутизации, такие как протоколы сбора маршрутной информации RIP (Routing Internet Protocol) и OSPF (Open Shortest Path First), а также протокол межсетевых управляющих сообщенийICMP (Internet Control Message Protocol). Последний протокол предназначен для обмена информацией об ошибках между маршрутизаторами сети и узлом - источником пакета. С помощью специальных пакетов ICMP сообщается о невозможности доставки пакета, о превышении времени жизни или продолжительности сборки пакета из фрагментов, об аномальных

величинах параметров, об изменении маршрута пересылки и типа обслуживания, о состоянии системы и т.п.

Следующий уровень (уровень II) называется основным. На этом уровне функционируют протокол управления передачей TCP (Transmission Control Protocol) и протокол дейтаграмм пользователя UDP (User Datagram Protocol). Протокол TCP обеспечивает надежную передачу сообщений между удаленными прикладными процессами за счет образования виртуальных соединений. Протокол UDP обеспечивает передачу прикладных пакетов дейтаграммным способом, как и IP, и выполняет только функции связующего звена между сетевым протоколом и многочисленными прикладными процессами.

Верхний уровень (уровень I) называется прикладным. За долгие годы использования в сетях различных стран и организаций стек TCP/IP накопил большое количество протоколов и сервисов прикладного уровня. К ним относятся такие широко используемые протоколы, как протокол копирования файлов FTP, протокол эмуляции терминала telnet, почтовый протокол SMTP, используемый в электронной почте сети Internet, гипертекстовые сервисы доступа к удаленной информации, такие как WWW и многие другие. Остановимся несколько подробнее на некоторых из них.

Протокол пересылки файлов FTP (File Transfer Protocol) реализует удаленный доступ к файлу. Для того, чтобы обеспечить надежную передачу, FTP использует в качестве транспорта протокол с установлением соединений - TCP. Кроме пересылки файлов протокол FTP предлагает и другие услуги. Так, пользователю предоставляется возможность интерактивной работы с удаленной машиной, например, он может распечатать содержимое ее каталогов. Наконец, FTP выполняет аутентификацию пользователей. Прежде, чем получить доступ к файлу, в соответствии с протоколом пользователи должны сообщить свое имя и пароль. Для доступа к публичным каталогам FTP-архивов Internet парольная аутентификация не требуется, и ее обходят за

счет использования для такого доступа предопределенного имени пользователя Anonymous.

В стеке TCP/IP протокол FTP предлагает наиболее широкий набор услуг для работы с файлами, однако он является и самым сложным для программирования. Приложения, которым не требуются все возможности FTP, могут использовать другой, более экономичный протокол - простейший протокол пересылки файловTFTP (Trivial File Transfer Protocol). Этот протокол реализует только передачу файлов, причем в качестве транспорта используется более простой, чем TCP, протокол без установления соединения - UDP.

Протокол telnet обеспечивает передачу потока байтов между процессами, а также между процессом и терминалом. Наиболее часто этот протокол используется для эмуляции терминала удаленного компьютера. При использовании сервиса telnet пользователь фактически управляет удаленным компьютером так же, как и локальный пользователь, поэтому такой вид доступа требует хорошей защиты. Поэтому серверы telnet всегда используют как минимум аутентификацию по паролю, а иногда и более мощные средства защиты, например, систему Kerberos.

Протокол SNMP (Simple Network Management Protocol) используется для организации сетевого управления. Изначально протокол SNMP был разработан для удаленного контроля и управления маршрутизаторами Internet, которые традиционно часто называют также шлюзами. С ростом популярности протокол SNMP стали применять и для управления любым коммуникационным оборудованием - концентраторами, мостами, сетевыми адаптерами и т.д. и т.п. Проблема управления в протоколе SNMP разделяется на две задачи.

Первая задача связана с передачей информации. Протоколы передачи управляющей информации определяют процедуру взаимодействия SNMP-

агента, работающего в управляемом оборудовании, и SNMP-монитора, работающего на компьютере администратора, который часто называют также консолью управления. Протоколы передачи определяют форматы сообщений, которыми обмениваются агенты и монитор.

Вторая задача связана с контролируемыми переменными, характеризующими состояние управляемого устройства. Стандарты регламентируют, какие данные должны сохраняться и накапливаться в устройствах, имена этих данных и синтаксис этих имен. В стандарте SNMP определена спецификация информационной базы данных управления сетью. Эта спецификация, известная как база данных MIB (Management Information Base), определяет те элементы данных, которые управляемое устройство должно сохранять, и допустимые операции над ними.

Протоколы этих уровней полностью реализуют функциональные возможности модели OSI. На стеке протоколов TCP/IP построено всё взаимодействие пользователей в IP-сетях. Стек является независимым от физической среды передачи данных[8].

1.4 Структурные схемы локальных сетей

Под структурной схемой сети понимается способ описания конфигурации сети, то есть ее топология. Топология - это конфигурация сети, способ соединения элементов сети (то есть компьютеров) друг с другом. Чаще всего встречаются три способа объединения компьютеров в локальную сеть: «звезда», «шина» и «кольцо»[14].

Сетевая топология может быть:

Физической – описывает реальное расположение и связи между узлами сети;

Логической – описывает хождение сигнала в рамках физической топологии;

Информационной – описывает направление потоков информации, передаваемых по сети;

Управления обменом – это принцип передачи права на пользование сетью.

1.4.1 Звезда

Звезда — базовая топология компьютерной сети, в которой каждый компьютер через специальный сетевой адаптер подключается к центральному узлу (обычно сетевой концентратор). При необходимости можно объединить вместе несколько сетей с топологией "звезда", при этом конфигурация сети получается разветвленной [14].

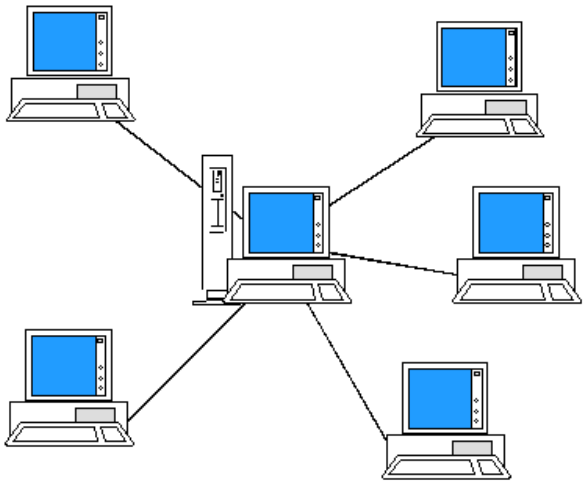


Рисунок 1.2 – Звездообразная топология сети

Рабочая станция, которой нужно послать данные, отсылает их на концентратор, а тот определяет адресата и отдаёт ему информацию. В определённый момент времени только одна машина в сети может пересылать данные, если на концентратор одновременно приходят два пакета, обе посылки оказываются не принятыми и отправителям нужно будет подождать случайный промежуток времени, чтобы возобновить передачу данных.

Достоинства: При соединении типа "звезда" легко искать неисправность в сети.

Недостатки: Соединение не всегда надежно, поскольку выход из строя центрального узла может привести к остановке сети.

1.4.2 Шина

Топология типа «Шина», представляет собой общий кабель (называемый шина или магистраль), к которому подсоединены все рабочие станции. На концах кабеля находятся терминаторы, для предотвращения отражения сигнала [8].

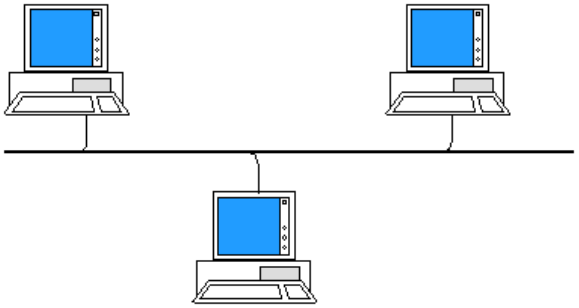


Рисунок 1.3 – Шинная топология сети

Отправляемое рабочей станцией сообщение распространяется на все компьютеры сети. Каждая машина проверяет — кому адресовано сообщение и если ей, то обрабатывает его. Для того, чтобы исключить одновременную посылку данных, применяется либо «несущий» сигнал, либо один из компьютеров является главным и «даёт слово» остальным станциям.

При построении больших сетей возникает проблема ограничения на длину связи между узлами, в таком случае сеть разбивают на сегменты. Сегменты соединяются различными устройствами — повторителями, концентраторами или хабами. Например, технология Ethernet позволяет использовать кабель длиной не более 185 метров.

Достоинства: в топологии "общая шина" выход из строя отдельных компьютеров не приводит всю сеть к остановке.

Недостатки: несколько труднее найти неисправность в кабеле и при обрыве кабеля (единого для всей сети) нарушается работа всей сети.

1.4.3 Кольцо

Кольцо - базовая топология компьютерной сети, в которой рабочие станции подключены последовательно друг к другу, образуя замкнутую сеть [14].

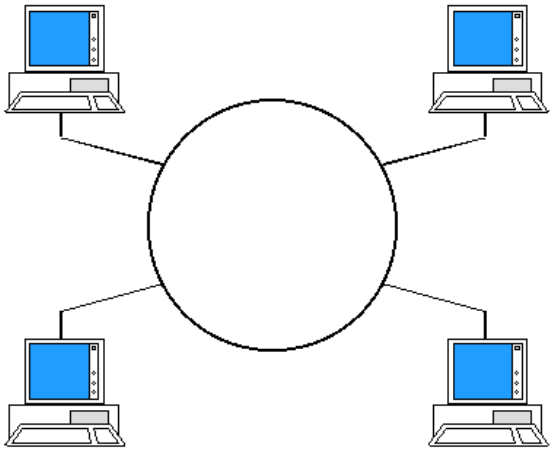


Рисунок 1.4 – Кольцевая топология сети

В кольце не используется конкурентный метод посылки данных, компьютер в сети получает данные от соседа и перенаправляет их дальше, если они адресованы не ему. Для определения того, кому можно передавать данные обычно используют маркер. Данные ходят по кругу, только в одном направлении.

Достоинства: балансировка нагрузки, возможность и удобство прокладки кабеля.

Недостатки: физические ограничения на общую протяженность сети.

Наиболее широкое применение получила в оптоволоконных сетях. Используется в стандартах FDDI, Token ring [13].

Топологию выбирают, исходя из потребностей предприятия. Если предприятие занимает многоэтажное здание, то в нем может быть применена схема "снежинка", в которой имеются файловые серверы для разных рабочих групп и один центральный сервер для всего предприятия.

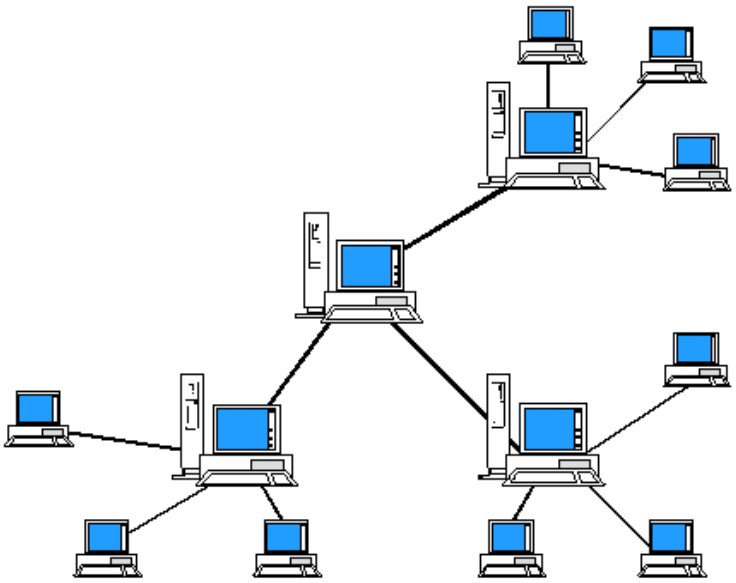


Рисунок 1.5 – Топология сети «снежинка»

1.5 Технология Fast Ethernet

Fast Ethernet — общее название для набора стандартов передачи данных в компьютерных сетях по технологии Ethernet со скоростью до 100 Мбит/с, в отличие от исходных 10 Мбит/с. Наиболее распространенная на данный момент технология связи [14].

Достоинства:

- увеличение пропускной способности сегментов сети до 100 Мбит/с;
- сохранение метода случайного доступа Ethernet;
- сохранение звездообразной топологии и поддержка традиционных средств передачи данных – витой пары и оптоволоконного кабеля.

Технология Fast Ethernet обладает свойством совместимости с другими технологиями и стандартами, что позволяет без проблем внедрять ее как в уже старые сети (Ethernet), так и в более новые (Wi-Fi).

Формат кадра остается неизменным и аналогичен кадру Ethernet [13].

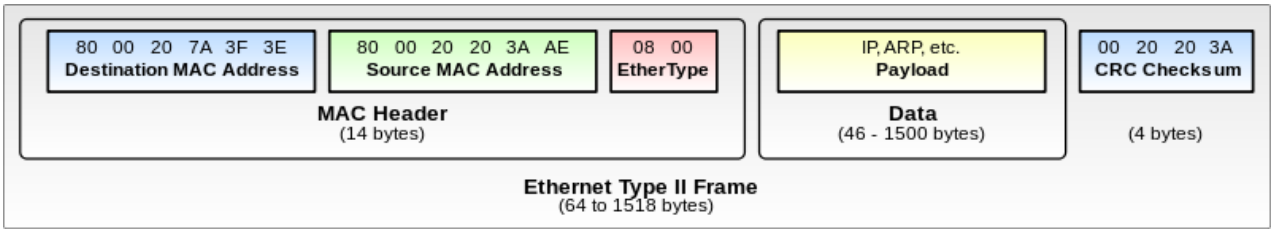


Рисунок 1.6 – Формат кадра Ethernet/Fast Ethernet

Существует множество вариантов реализации данной технологии, наиболее популярными из которых являются:

- 100BASE-FX — вариант Fast Ethernet с использованием волоконно-оптического кабеля. В данном стандарте используется длинноволновая часть спектра (1300 нм) передаваемая по двум жилам, одна для приёма (RX) и одна для передачи (TX). Длина сегмента сети может достигать 400 метров (1 310 футов) в полудуплексном режиме (с гарантией обнаружения коллизий) и двух километров (6 600 футов) в полнодуплексном при использовании многомодового волокна. Работа на больших расстояниях возможна при использовании одномодового волокна. 100BASE-FX не совместим с 10BASE-FL, 10 Мбит/с вариантом по волокну.
- 100BASE-SX — удешевленная альтернатива 100BASE-FX с использованием многомодового волокна, так как использует недорогую коротковолновую оптику. 100BASE-SX может работать на расстояниях до 300 метров (980 футов). 100BASE-SX использует ту же самую длину волны как и 10BASE-FL. В отличие от 100BASE-FX, это позволяет 100BASE-SX быть обратно-совместимым с 10BASE-FL. Благодаря использованию более коротких волн (850 нм) и небольшой дистанции, на которой он может работать, 100BASE-SX использует менее дорогие оптические компоненты (светодиоды (LED) вместо лазеров). Все это делает данный стандарт привлекательным для тех, кто

модернизирует сеть 10BASE-FL и тех, кому не нужна работа на больших расстояниях.

- 100BASE-BX — вариант Fast Ethernet по одножильному волокну. Используется одномодовое волокно, наряду со специальным мультиплексором, который разбивает сигнал на передающие и принимающие волны.
- 100BASE-LX — 100 Мбит/с Ethernet с помощью оптического кабеля. Максимальная длина сегмента 15 километров в полнодуплексном режиме по паре одномодовых оптических волокон.
- 100BASE-LX WDM — 100 Мбит/с Ethernet с помощью волоконно-оптического кабеля. Максимальная длина сегмента 15 километров в полнодуплексном режиме по одному одномодовому оптическому волокну на длине волны 1310 нм и 1550 нм. Интерфейсы бывают двух видов, отличаются длиной волны передатчика и маркируются либо цифрами (длина волны), либо одной латинской буквой A(1310) или B(1550). В паре могут работать только парные интерфейсы: с одной стороны передатчик на 1310 нм, а с другой — на 1550 нм.
- 100BASE-TX – 100 Мбит/с Ethernet с помощью витой пары. Длина сегмента кабеля ограничена 100 метрами.

Поскольку целью данной дипломной работы является разработка локальной сети предприятия, вариант реализации 100BASE-TX является наиболее оптимальным, как с качественной, так и с экономической стороны [14].

1.5.1 Протоколы сети

Протокол – это набор правил и технических процедур, регулирующих осуществления связи между компьютерами в сети [13].

Стек протоколов – это комбинация протоколов, работающих на одном компьютере.

Задачей протоколов является определение таких шагов и контроль за их выполнением. Например, если два протокола будут по-разному разбивать данные на пакеты и добавлять к ним служебную информацию, тогда компьютер, использующий один из этих протоколов, не сможет успешно связаться с компьютером, на котором работает другой протокол [13].

Протоколы делятся на прикладные, транспортные и сетевые.

Прикладные – обеспечивают взаимодействие приложений на разных компьютерах между собой. К наиболее популярным относятся:

- SMTP (Simple Mail Transfer Protocol) – протокол Интернета для обмена электронной почтой;
- FTP (File Transfer Protocol) – протокол Интернета для передачи файлов;
- Telnet – протокол Интернета для обработки данных на удаленных компьютерах и т.д.

Транспортные – поддерживают сеансы связи между компьютерами, определяют маршрут следования пакетов и гарантируют надежный обмен данными. К ним относятся:

- TCP – часть набора протокола TCPЛP, служащий для гарантированной доставки сообщений, разбитых на пакеты;
- SPX – часть набора протокола IPX/SPX (InternetworkPacket Exchange/SeqLlential Packet Exchange) фирмы Novell для данных, разбитых на пакеты;
- NetBEUI (NetBIOS Extended User Interface – расширенный интерфейс пользователя) - устанавливает сеансы связи между компьютерами.

Сетевые – управляют функциями адресации, маршрутизации, проверки ошибок и Т.д., а также определяют правила для осуществления связи в конкретных сетевых средах (например, Ethernet или Token Ring). К ним относятся следующие протоколы:

- IP (Internet Protocol) - протокол для передачи пакетов в сети Интернет (обычно используется комбинация протоколов TCP/IP);
- IPX (Internetwork Packet Exchange) - протокол фирмы NetWare для передачи и маршрутизации пакетов;
- NetBEUI – используется как транспортный, так и сетевой протокол.

Для данной сети будет использоваться комбинация TCP/IP протоколов. Данные протоколы является наиболее известными и чаще употребляемые в ЛВС [13].

1.6 Технология VPN и удаленный доступ

VPN – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений, передаваемых по логической сети сообщений) [14].

В зависимости от применяемых протоколов и назначений, VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть.

Связь с удалённой локальной сетью, подключенной к глобальной сети, из дома/командировки/удалённого офиса часто реализуется через VPN. При этом устанавливается VPN-подключение к пограничному маршрутизатору.

Особенно популярен следующий способ организации удалённого доступа к локальной сети:

- обеспечивается подключение снаружи к маршрутизатору, например по протоколу PPPoE, PPTP или L2TP (PPTP+IPSec).
- так как в этих протоколах используется PPP, то существует возможность назначить абоненту IP-адрес. Назначается свободный (не занятый) IP-адрес из локальной сети.
- маршрутизатор (VPN, Dial-in сервер) добавляет proxyarp — запись на локальной сетевой карте для IP-адреса, который он выдал VPN-клиенту. После этого, если локальные компьютеры попытаются обратиться напрямую к выданному адресу, то они после ARP-запроса получат MAC-адрес локальной сетевой карты сервера и трафик пойдёт на сервер, а потом и в VPN-туннель.

1.7 Технология IP-телефонии

Под IP телефонией понимается технология передачи голоса и факс сообщений через сети, использующие протокол IP, в режиме реального времени. Данный протокол используется как в сети Интернет, так и в локальных сетях. Технология IP телефонии объединяет сети с коммутацией каналов (передающие голосовую информацию) и сети с коммутацией пакетов (передающие данные) в единую коммуникационную сеть. Бесперебойное распознавание голоса и его передача из одной сети в другую решается с помощью различных шлюзов. Шлюз представляет собой устройство, в которое с одной стороны включаются телефонные линии, а с другой стороны - IP-сеть.

Голос, как аналоговые колебания в системе IP телефонии, существует только в телефонной трубке, или в том, что заменяет ее. На остальных участках канала передачи от абонента к абоненту речь оцифровывается и передается в виде IP пакетов. Пакеты данных имеют в своем составе порядковый номер, адреса точек назначения (приема и передачи) и информацию для коррекции ошибок. Для того чтобы пакеты были направлены

нужному получателю используется IP адрес, в соответствии с которым осуществляется их маршрутизация. Узлы IP направляют эти пакеты по сети до окончания маршрута доставки. Пакеты, приходящие на ближайший к другому абоненту шлюзу, преобразовываются обратно в аналоговый вид (голосовой сигнал) и поступают в телефонную линию.

1.7.1 Протоколы IP-телефонии

H.323 - основополагающий стандарт, принятый ITU-T, где описывается, каким образом чувствительный к задержке трафик, в частности голос и видео, получает приоритет в локальных и глобальных сетях. Он состоит из ряда рекомендаций (стека протоколов) по смежным техническим вопросам, таким, как качество речи, стандарты кодирования звуковой и видеоинформации и пр. Протокол SIP (Session Initiation Protocol) в большей степени соответствует идеологии TCP/IP, чем стек протоколов H.323. О поддержке этого протокола заявили такие производители как 3Com, Cisco, Ericsson, Siemens. Однозначность стандарта SIP позволяет с уверенностью говорить о совместимости IP-шлюзов разных производителей.

1.7.2 Алгоритмы сжатия звука

Для кодирования звуковой информации обычно используются следующие кодеки: G.711, G.722, GSM0610, G.723, G.723.1, G.728, и G.729. Для кодека G.711 требуется ширина полосы частот в 64 Кбит/с, поэтому он приемлем не во всех IP-сетях (например, в Интернет), т.к. большинство пользователей Интернета имеет канал заведомо меньшей ширины. Кодеки с

низкой шириной полосы частот - G.729 в 8 Кбит/с и G.723.1 в 5.3/6.3 Кбит/с - вполне подходят для использования в Интернет. В частности, G.723.1 является одним из нескольких "стандартных" кодеков для IP-телефонии, особенно после того, как Intel, Microsoft и Netscape объявили о поддержке этого стандарта звукового кодирования.

1.8 Технология Wi-Fi

Wi-Fi — (Wireless Fidelity) так называют один из стандартов беспроводной передачи данных, а точнее, стандарт IEEE 802.11b. Он входит в группу из 8 стандартов беспроводной передачи данных, из которых технически реализованы только два — 802.11a и 802.11b. Беспроводные сети отличаются от кабельных сетей на физическом (Phy) и частично на канальном (MAC) – уровнях модели взаимодействия OSI.

Физический уровень IEEE 802.11x - радиоканал. Этот уровень характеризует параметры физической среды передачи данных. Стандарт IEEE 802.11x обеспечивает передачу сигнала, несущего информацию, одним из методов: прямой последовательности (DSSS - Direct Sequence Spread Spectrum) и частотных скачков (FHSS - Frequency Hopping Spread Spectrum). Эти методы отличаются способом модуляции, но используют одинаковую технологию расширения спектра.

Канальный уровень. Канальный уровень осуществляет управление доступом к передающей среде и обеспечивает пересылку кадров между любыми двумя устройствами беспроводной сети. Канальный уровень разделяется на два подуровня: MAC - управление доступом к среде передачи данных и LCC - управление логическим каналом.

Скорость передачи данных для Wireless оборудования, поддерживающего стандарт 802.11b, не превышает 11 Мбит/с, а для оборудования, поддерживающего стандарт 802.11g, до 54 Мбит/с. Стандарт

802.11n способен обеспечить скорость передачи данных до 600 Мбит/с. Для 802.11a скорость передачи данных - 54 Мбит/с.

Для работы в стандарте 802.11x используется оборудование двух основных типов: точка доступа Access Point и клиенты, к которым относятся различные устройства, оборудованные Wi-Fi - адаптерами. Access Point - это программно-аппаратное устройство, которое состоит из приемопередатчика, выполняющего роль беспроводного сетевого концентратора (интерфейса для клиентов беспроводной сети - WLAN), сетевого адаптера (интерфейса проводной сети) для подключения к кабельной сети LAN или WAN и микроконтроллера для обработки данных.

1.8.1 Создания беспроводных локальных сетей

Существует два основных способа организации беспроводной локальной сети (WLAN) – это режимы инфраструктуры (Infrastructure Mode) и точка-точка (Adhoc).

В беспроводной локальной сети, функционирующей в режиме Infrastructure Mode (в инфраструктурном режиме Wi-Fi), беспроводные устройства общаются между собой через точку доступа Access Point. Точка доступа передаёт идентификатор сети SSID (Service Set ID) с помощью специальных сигнальных пакетов. Беспроводные устройства подключаются к Access Point, используя ее идентификатор сети SSID, и обмениваются информацией друг с другом. В этом случае Access Point используется в качестве центральной точки подключения беспроводных устройств.

В беспроводной локальной сети типа Adhoc связь устанавливается непосредственно между устройствами, оборудованными Wi-Fi- адаптерами, и в этом случае точка доступа вообще не используется. Режим "Adhoc" - это режим "равный-с-равным" (peer-to-peer).

1.8.2 Организация доступа к Интернету

Технология Wi-Fi может обеспечить доступ к ресурсам сети Интернет по беспроводному протоколу радиодоступа Wi-Fi в радиусе действия точки доступа. Такие общественные точки доступа называются Hotspot или местом, где имеется высокоскоростной беспроводный доступ в сеть Интернет.

Хотспот или публичная зона беспроводного доступа — это территория (помещения вокзала, офиса, учебных аудиторий, кафе и т.д.), покрытая беспроводной сетью Wi-Fi, на которой пользователь, имеющий устройство с беспроводным адаптером стандарта Wi-Fi, может подключиться к Интернет.

Для расширения зоны радиопокрытия Hotspot или увеличения радиуса действия беспроводной сети можно устанавливать репитеры (ретрансляторы Wi-Fi) через какое-то расстояние от базовой точки доступа, которые будут повторять сигнал базовой точки доступа. В общем случае для организации хотспота точка доступа подключается к провайдеру, используя один из стандартных способов: технологию ADSL, 3G или локальную сеть Fast Ethernet.

2 КОНСТРУКТОРСКАЯ ЧАСТЬ

2.1 Планирование сети

При разработке и проектировании сети необходимо в первую очередь составить план, включающий в себя список VLAN, план IP-адресации и план интерфейсов.

Список VLAN содержит в себе полный перечень настраиваемых виртуальных локальных сетей, включая резервные. Необходим для упрощения настройки, поскольку запоминание абсолютно всех VLAN и соответствующих им параметров затруднительно.

Таблица 2.1 – Список VLAN

№ VLAN	Имя VLAN	Примечание
1	default	Не используется
2	Management	Для управления
3	Servers	Сервера
4 – 100		Зарезервировано
101	PTO	Для пользователей ПТО
102	FEO	Для пользователей ФЭО
103	Accounting	Бухгалтерия
104	Other	Другие пользователи

План IP-адресации содержит адреса шлюзов, а так же пулов раздачи для каждого VLAN. Так же в этот план входят IP-адреса коммутаторов, маршрутизаторов и прочих сетевых устройств, включая сервера.

Таблица 2.2 – План IP-адресации

IP-адрес	Назначение	VLAN
172.16.0.0/16		
172.16.0.0/24	Серверная ферма	3
172.16.0.1	Шлюз	
172.16.0.2	File-server	
172.16.0.3 – 172.16.0.254	Зарезервировано	
172.16.1.0/24	Управление	2
172.16.1.1	Шлюз	
172.16.1.2	DSW2	
172.16.1.3	ASW1	
172.16.1.4	ASW3	
172.16.1.5	ASW2	
172.16.1.6 – 172.16.1.254	Зарезервировано	
172.16.2.0/24	Сеть Point-to-point	
172.16.2.1	Шлюз	
172.16.2.2 – 172.16.2.254	Зарезервировано	
172.16.3.0/24	ПТО	101
172.16.3.1	Шлюз	
172.16.3.2 – 172.16.3.254	Зарезервировано	
172.16.4.0/24	ФЭО	102
172.16.4.1	Шлюз	
172.16.4.2 – 172.16.4.254	Зарезервировано	
172.16.5.0/24	Бухгалтерия	103
172.16.5.1	Шлюз	
172.16.5.2 – 172.16.5.254	Зарезервировано	
172.16.6.0/24	Другие	104
172.16.6.1	Шлюз	
172.16.6.2 – 172.16.6.254	Зарезервировано	

Таблица 2.3 – План интерфейсов

Имя устройства	Порт	Название	VLAN	
			Access	Trunk
DSW1	FE0/1	provider		2,3,6,101-104
	GE0/1	DSW2		2,3
	GE0/2	ASW3		2,101-104
	FE0/24	ASW1		2,101,104
DSW2	GE1/1	DSW1		2,3
	GE1/2	ASW2		2,3
ASW1	FE0/24	DSW1		2,101,104
	FE0/1 – 0/12	PTO	101	
	FE0/13 – 0/20	Other	104	
ASW3	GE1/1	DSW1		2,101-104
	FE0/1 – 0/5	PTO	101	
	FE0/6 – 0/10	FEO	102	
	FE0/11 – 0/15	Accounting	103	
	FE0/16 – 0/24	Other	104	
ASW2	GE1/1	DSW2		2,3
	FE0/1 – 0/20	Servers	3	
	GE1/2	File-server	3	

План интерфейсов необходим для четкого понимания, какие порты относятся к определенным VLAN, какие порты сетевых устройств должны быть соединены между собой и трафик каких VLAN должен передаваться между этими устройствами через указанные интерфейсы.

Имея все три необходимых плана, и зная как подключать и соединять оборудование, можно приступать к рассмотрению используемого оборудования.

2.2 Сетевое оборудование

Оборудование производится компанией Cisco и является универсальным решением для большинства задач построения сетей.

Для сетей средних и крупных размеров идеально подойдут коммутаторы Cisco серии Catalyst 2960-24LT-L, имеющие 24 Fast Ethernet порта для конечных пользователей и 2 Gigabit Ethernet порта для магистральных соединений [17].

Рисунок 2.1 – Коммутатор Cisco Catalyst 2960-24LT-L

К особенностям коммутаторов серии 2960 относятся:

- универсальность: поддержка передачи данных, беспроводной и голосовой связи. Когда вам понадобятся все эти функции, при выборе данного коммутатора вы получите единую сеть, отвечающую всем потребностям вашей организации;
- интеллектуальное управление: назначение приоритета голосовому трафику или передаче данных с целью согласовать доставку информации с потребностями организации;
- повышенная безопасность: защита информации, предотвращение доступа к сети неавторизованных пользователей и обеспечение бесперебойной работы;

- надежность: использование преимуществ стандартных методов и модуля стекирования FlexStack для повышения надежности и быстрого устранения неполадок. Для дополнительного повышения надежности можно также добавить резервный источник питания;
- удобство настройки конфигурации: использование набора функций Cisco Catalyst Smart Operations и приложения Cisco Network Assistant для упрощения настройки, обновления и устранения неполадок;
- залог спокойствия: все коммутаторы Catalyst серий 2960, 2960-C и 2960-S защищены ограниченной гарантией Cisco, действующей в течение всего срока службы оборудования, и отсутствием ограничений на обновления.

Однако их использование ограничивается уровнем доступа и распределения. Поэтому для спаренного уровня ядра и распределения понадобится использовать более мощный коммутатор – Cisco Catalyst 3560-24PS-S [17].

Рисунок 2.2 – Коммутатор Cisco Catalyst 3560-24PS-S

Как и 2960-24LT-L он имеет 24 Fast Ethernet и 2 Gigabit Ethernet порта, однако его возможности куда шире, чем у обычного коммутатора. 3560-24PS-S поддерживает большинство функции маршрутизаторов и идеально подходит как многоуровневый коммутатор [17].

К особенностям серии 3560 относятся:
- высокоскоростная маршрутизация трафика: благодаря технологии Cisco Express Forwarding (CEF) серия Catalyst 3560 обеспечивает высокопроизводительную маршрутизацию трафика IP. Программное

обеспечение SMI поддерживает статическую, RIPv1 и RIPv2 маршрутизацию, а EMI – еще и OSPF, IGRP, EIGRP, а также маршрутизацию multicast трафика (PIM, DVMRP, IGMP snooping);

- высокая безопасность: поддержка протокола 802.1x, функциональность Identity-Based Networking Services (IBNS), списки доступа для трафика, коммутируемого на втором уровне (VLAN ACL), на третьем и четвертом уровнях (Router ACL), а также Port-based ACLs (PACL) и Time-based ACL. Для обеспечения безопасности при администрировании поддерживаются протоколы SSH и SNMPv3, а также централизованная аутентификация на TACACS+ и RADIUS серверах;
- высокая доступность: для защиты от сбоев внутренних блоков питания коммутаторы Catalyst 3560 поддерживают резервную систему питания Cisco Redundant Power System 675 (RPS 675), протоколы 802.1D, 802.1s, 802.1w, функциональность UplinkFast, HSRP, UDLD, Aggressive UDLD, Switch port Auto-recovery;
- поддержка качества обслуживания (QoS):классификация трафика по полям DSCP или 802.1p (CoS), стандартные и расширенные списки доступа для выделения заданного типа трафика, WRED, очередность Strict Priority, Shaped Round Robin. Существует возможность определения максимальной полосы для определенного вида трафика, а также выделения гарантированной полосы CIR;
- отличная управляемость: внедренное в коммутатор ПО Cisco CMS, поддержка управления с помощью SNMP-платформ, таких как CiscoWorks, поддержка SNMP версий 1, 2, 3, Telnet, RMON, SPAN, RSPAN, NTP, TFTP.

2.3 Логическая топология сети

При построении сетей средних и крупных размеров используется так называемая иерархическая модель сети, где коммутаторы и маршрутизаторы относятся к одному из трех уровней и выполняют функции, относящиеся именно к этому уровню.

На самом низком уровне находятся коммутаторы уровня доступа (Access Layer Switch, ASW). К ним подключаются конечные пользователи.

Уровнем выше находятся коммутаторы уровня распределения (Distribution Layer Switch, DSW). Они обеспечивают высокоскоростной обмен данными между пользователями, не подключенными к одному коммутатору уровня доступа.

Самым высоким уровнем является уровень ядра (Core Layer). Оборудование этого уровня обеспечивает связь с другими локальными сетями, в том числе Интернет [17].

В рамках данной дипломной работы Core Layer можно объединить с Distribution Layer, используя многоуровневый коммутатор.

Логическая топология сети без учета хостов и с обозначением интерфейсов будет выглядеть следующим образом:

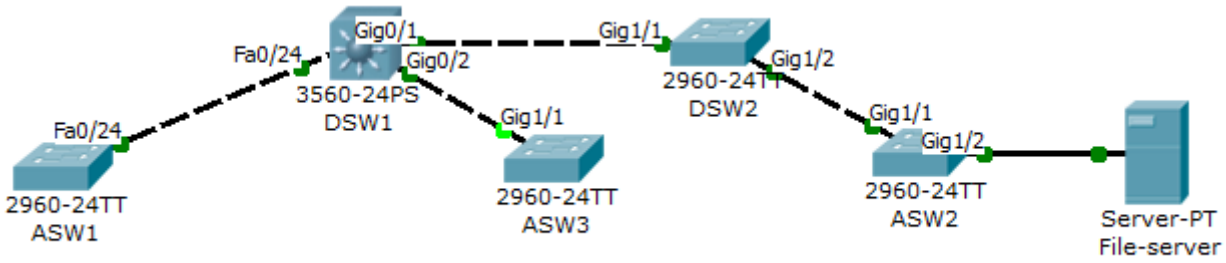


Рисунок 2.3 – Логическая топология сети

Каждый коммутатор уровня доступа образует «звезду», а все вместе они объединены в «дерево».

3 ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

3.1 Среда моделирования

Моделирование и настройка сети производится в программе Cisco Packet Tracer версии 5.3.3, позволяющей делать работоспособные модели сетей, производить их настройку командами Cisco IOS, взаимодействовать между пользователями. Включает в себя серверы DHCP, HTTP, TFTP, FTP, рабочие станции, различные модули к компьютерам и маршрутизаторам [17].

Успешно позволяет создавать даже сложные макеты сетей и проверять на работоспособность топологии.

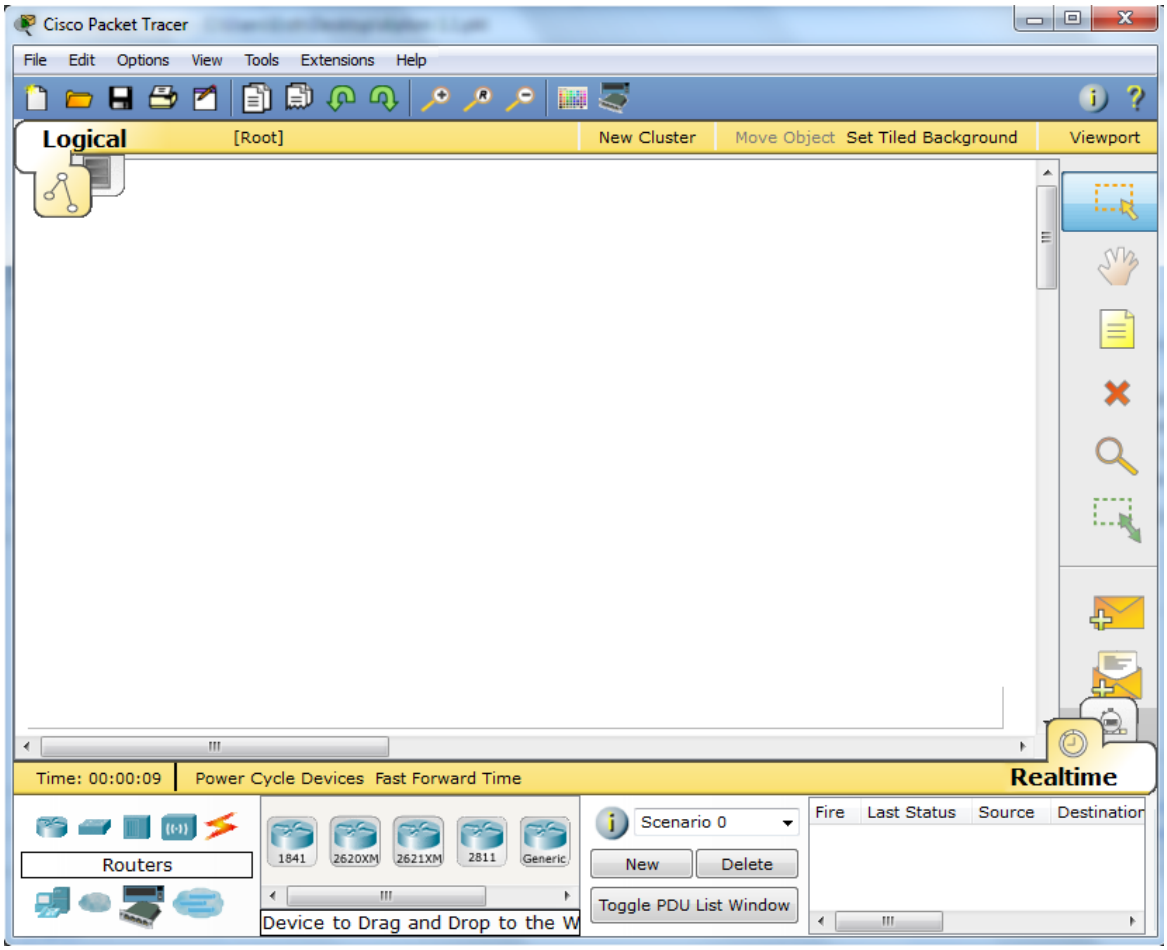


Рисунок 3.1 – Рабочее окно Cisco Packet Tracer

3.2 Листинг настройки

3.2.1 Настройка коммутаторов уровня доступа

В первую очередь настраивается коммутатор ASW1.

```
/* Задаем имя устройству */;
>enable
#configure terminal
#hostname ASW1
/* Создаем все VLAN’ы */;
#vlan 2
#name Management
#vlan 101
#name PTO
#vlan 104
#name Other
/* Настраиваем access-порты */;
#interface range fastEthernet 0/1-12
#description PTO
#switchport mode access
#switchport access vlan 101
#exit
#interface range fastEthernet 0/13-20
#description Other
#switchport mode access
#switchport access vlan 104
#exit
/* Настраиваем trunk-порт */;
```

#interface fastEthernet 0/24

#description DSW1

#switchport mode trunk

#switchport trunk allowed vlan 2,101,104

#exit

/* Настраиваем сеть управления */;

#interface vlan 2

#ip address 172.16.1.3 255.255.255.0

#ip default-gateway 172.16.1.1

#exit

/* Сохранение */;

#copy running-config startup-config

Следующим настраивается ASW2

/* Задаем имя устройству */

>enable

#configure terminal

#hostname ASW2

/* Создаем все VLAN’ы */;

#vlan 2

#name Management

#vlan 3

#name Servers

/*Настраиваем access-порты*/

#interface range fastEthernet 0/1-20

#description Servers

#switchport mode access

#switchport access vlan 3

#exit

#interface GigabitEthernet 1/2

#description Servers

#switchport mode access

#switchport access vlan 3

#exit

/*Настраиваем trunk-порт*/

#interface GigabitEthernet 1/1

#description DSW2

#switchport mode trunk

#switchport trunk allowed vlan 2,3

#exit

/*Настраиваем сеть управления*/

#interface vlan 2

#ip address 172.16.1.5 255.255.255.0

#ip default-gateway 172.16.1.1

#exit

/*Сохранение*/

#copy running-config startup-config

В последнюю очередь настраивается ASW3, требующий больше времени на изменение конфигурации.

/* Задаем имя устройству */

>enable

#configure terminal

#hostname ASW3

/* Создаем все VLAN’ы */;

#vlan 2

#name Management

#vlan 101

#name PTO

#vlan 102

```
#name FEO
#vlan 103
#name Accounting
#vlan 104
#name Other
/* Настраиваем access-порты */;
#interface range fastEthernet 0/1-5
#description PTO
#switchport mode access
#switchport access vlan 101
#exit
#interface range fastEthernet 0/6-10
#description FEO
#switchport mode access
#switchport access vlan 102
#exit
#interface range fastEthernet 0/11-15
#description Accounting
#switchport mode access
#switchport access vlan 103
#exit
#interface range fastEthernet 0/16-24
#description Other
#switchport mode access
#switchport access vlan 104
#exit
/* Настраиваем trunk-порт */;
#interface GigabitEthernet 1/1
#description DSW1
#switchport mode trunk
```

#switchport trunk allowed vlan 2,101-104

#exit

/* Настраиваем сеть управления */;

#interface vlan 2

#ip address 172.16.1.4 255.255.255.0

#ip default-gateway 172.16.1.1

#exit

/* Сохранение */;

#copy running-config startup-config

3.2.2 Настройка коммутаторов уровня распределения

В первую очередь настраивается DSW2, поскольку он выполняет только функции распределения и его настройка не отнимает много времени.

/* Задаем имя устройству */;

>enable

#configure terminal

#hostname DSW2

/* Создаем все VLAN’ы */;

#vlan 2

#name Management

#vlan 3

#name Servers

/* Настраиваем trunk-порты */;

#interface range GigabitEthernet 1/1-1/2

#switchport mode trunk

#switchport trunk allowed vlan 2,3

#exit

/* Настраиваем сеть управления */;

#interface vlan 2

#ip address 172.16.1.2 255.255.255.0

#ip default-gateway 172.16.1.1

#exit

/* Сохранение */;

#copy running-config startup-config

Последним настраивается DSW1, являющийся спаренным коммутатором уровня распределения и ядра и требующий наиболее детальной настройки.

/* Задаем имя устройству: */;

>enable

#configure terminal

#hostname DSW1

/* Создаем все VLAN’ы */;

#vlan 2

#name Management

#vlan 3

#name Servers

#vlan 101

#name PTO

#vlan 102

#name FEO

#vlan 103

#name Accounting

#vlan 104

#name Other

/* Создаем VLAN для выхода в Internet */;

#vlan 6

```
#name Internet
/* Настраиваем trunk-порты */;
#interface GigabitEthernet 0/1
#description DSW2
#switchport trunk allowed vlan 2,3
#exit
#interface GigabitEthernet 0/2
#description ASW3
#switchport trunk allowed vlan 2,101-104
#exit
#interface fastEthernet 0/24
#description ASW1
#switchport trunk allowed vlan 2,101,104
#exit
/* Создаем VLAN-интерфейсы */;
#interface vlan 2
#ip address 172.16.1.1 255.255.255.0
#exit
#interface vlan 3
#ip address 172.16.0.1 255.255.255.0
#exit
#interface vlan 101
#ip address 172.16.3.1 255.255.255.0
#exit
#interface vlan 102
#ip address 172.16.4.1 255.255.255.0
#exit
#interface vlan 103
#ip address 172.16.5.1 255.255.255.0
#exit
```

```
#interface vlan 104
#ip address 172.16.6.1 255.255.255.0
#exit
/* Включаем маршрутизацию */;
#ip routing
/* Настраиваем DHCP-сервер */;
/* Исключаем адреса шлюзов из раздачи */;
#ip dhcp excluded-address 172.16.3.1
#ip dhcp excluded-address 172.16.4.1
#ip dhcp excluded-address 172.16.5.1
#ip dhcp excluded-address 172.16.6.1
/* Прописываем пулы адресов для раздачи */;
#ip dhcp pool PTO
#network 172.16.3.0 255.255.255.0
#default-router 172.16.3.1
#ip dhcp pool FEO
#network 172.16.4.0 255.255.255.0
#default-router 172.16.4.1
#ip dhcp pool Accounting
#network 172.16.5.0 255.255.255.0
#default-router 172.16.5.1
#ip dhcp pool Other
#network 172.16.6.0 255.255.255.0
#default-router 172.16.6.1
/* Сохранение */;
#copy running-config startup-config
```

После проведенных настроек все компьютеры сети будут «видеть» друг друга, подключаться к FTP-серверу, но не иметь выхода в Интернет.

На данный момент логическая топология сети выглядит следующим образом:

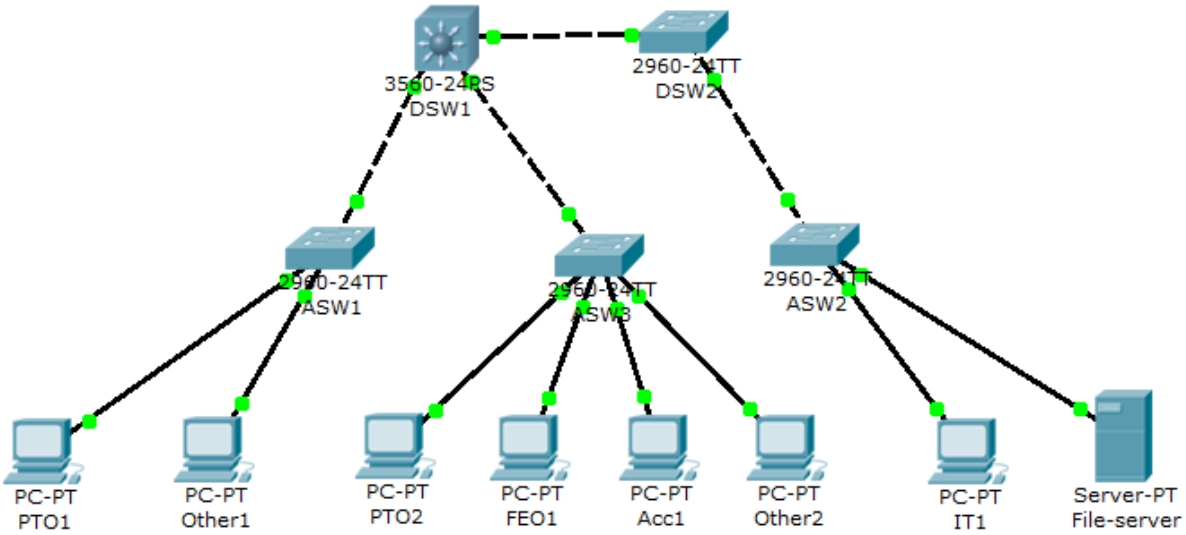


Рисунок 3.2 – Настраиваемая сеть

Компьютер PTO1 (VLAN 101), имеющий IP-адрес 172.16.3.2, «видит» компьютер PTO2, имеющий IP-адрес 172.16.3.3, из того же VLAN, находящегося в другом сегменте сети.

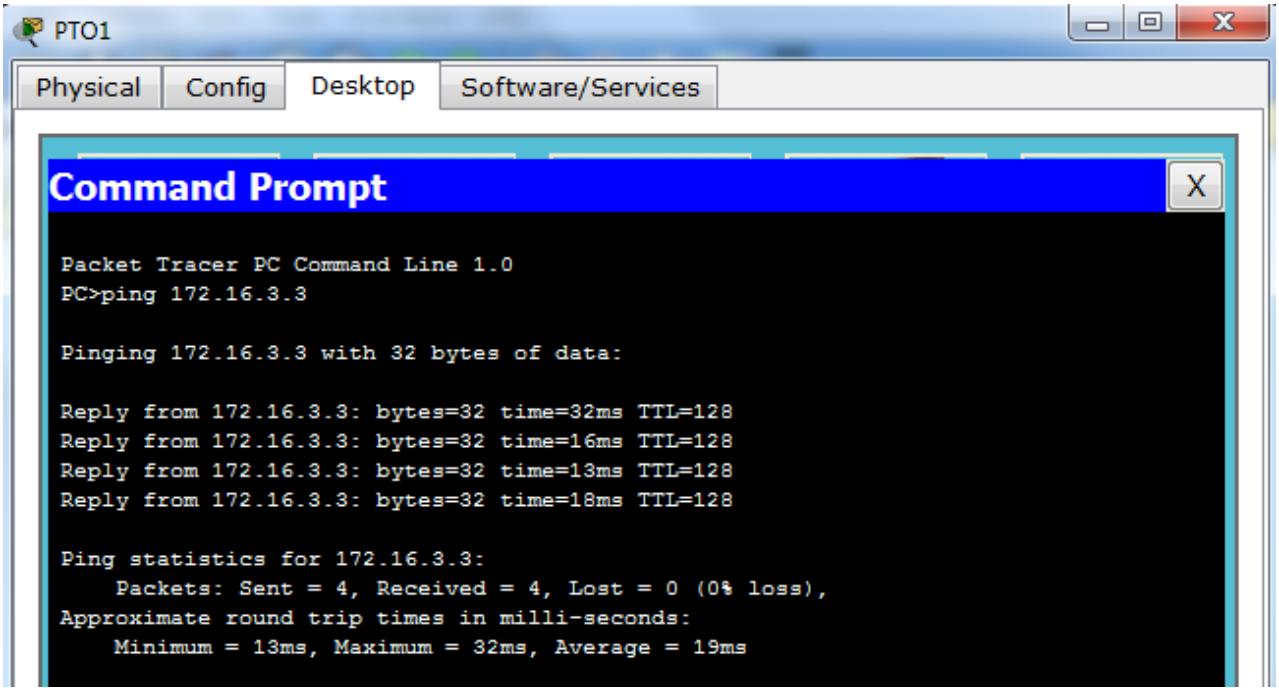


Рисунок 3.3 – Проверка связи между компьютерами PTO1 и PTO2

Аналогично будет проходить пинг и с компьютерами из других VLAN.

```
PC>ping 172.16.6.2

Pinging 172.16.6.2 with 32 bytes of data:

Reply from 172.16.6.2: bytes=32 time=18ms TTL=127
Reply from 172.16.6.2: bytes=32 time=14ms TTL=127
Reply from 172.16.6.2: bytes=32 time=17ms TTL=127
Reply from 172.16.6.2: bytes=32 time=14ms TTL=127

Ping statistics for 172.16.6.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 18ms, Average = 15ms
```

Рисунок 3.4 – Проверка связи между компьютером PTO1 и Other1 (172.16.6.2)

```
PC>ping 172.16.4.2

Pinging 172.16.4.2 with 32 bytes of data:

Reply from 172.16.4.2: bytes=32 time=13ms TTL=127
Reply from 172.16.4.2: bytes=32 time=16ms TTL=127
Reply from 172.16.4.2: bytes=32 time=17ms TTL=127
Reply from 172.16.4.2: bytes=32 time=7ms TTL=127

Ping statistics for 172.16.4.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 17ms, Average = 13ms
```

Рисунок 3.5 – Проверка связи между компьютером PTO1 и FEO (172.16.4.2)

```
Pinging 172.16.5.2 with 32 bytes of data:

Reply from 172.16.5.2: bytes=32 time=19ms TTL=127
Reply from 172.16.5.2: bytes=32 time=15ms TTL=127
Reply from 172.16.5.2: bytes=32 time=18ms TTL=127
Reply from 172.16.5.2: bytes=32 time=14ms TTL=127

Ping statistics for 172.16.5.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 19ms, Average = 16ms
```

Рисунок 3.4 – Проверка связи между компьютером PTO1 и Acc1 (172.16.5.2)

Файловый сервер и вся сеть VLAN 3 находится в отдельном сегменте, поскольку требует защиты от злоумышленников. Поэтому связь с данным сегментом сети не рассматривается.

3.3 Защита информации на файловом сервере

Необходимый уровень защиты информации обеспечивается благодаря спискам контроля доступа (ACL), настраиваемых на маршрутизаторах уровня ядра.

Поскольку в данной сети уровень ядра и распределения объединен в один коммутатор DSW1, все необходимые настройки ACL будут производиться на нем.

Для этого необходимо создать расширенный (extended) список доступа (ACL) с блокировкой всех портов за исключением 20, 21 и повесить его на соответствующий данному серверу интерфейс (VLAN 3) с фильтрацией исходящего трафика.

```
# configure terminal
#ip access-list extended Servers-out
#permit icmp any any
#permit tcp 172.16.0.0 0.0.255.255 host 172.16.0.2 range 20 21
#exit
#interface vlan 3
#ip access-group Servers-out out
```

3.4 Настройка доступа в Интернет

Все настройки производятся на коммутаторе DSW1.

```
#configure terminal
#interface vlan 6
#ip address 198.51.100.2 255.255.255.0
```

#exit

#ip route 0.0.0.0 0.0.0.0 198.51.100.1

Номер используемого VLAN и IP-адреса обговариваются с провайдером. Приведенные числа взяты для удобства.

Связь разрабатываемой сети с сетью провайдера условно выглядит следующим образом.

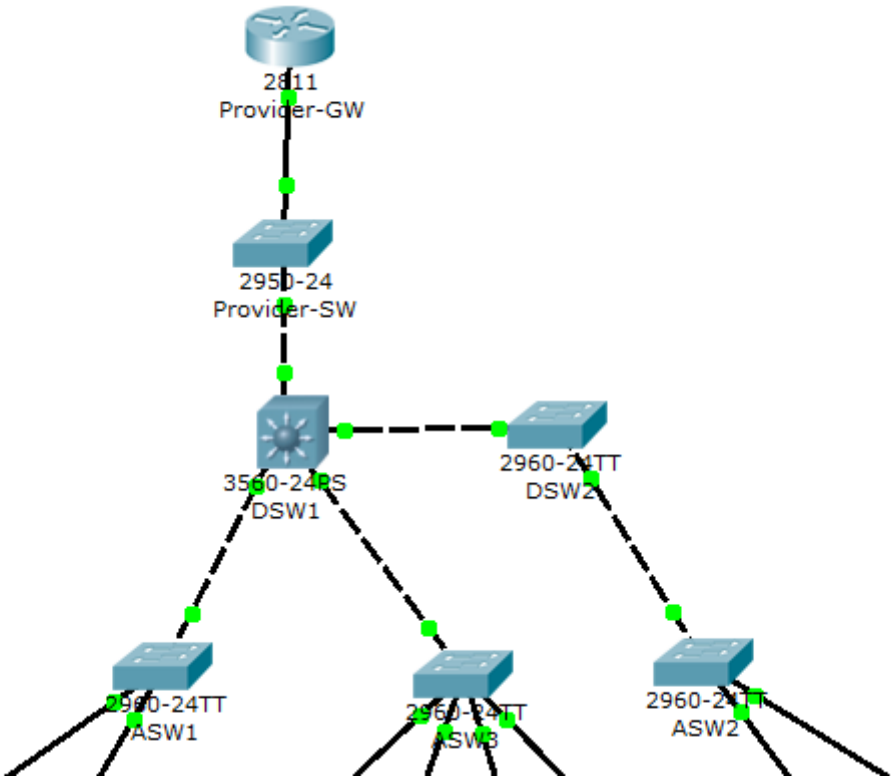


Рисунок 3.5 – Условная топология с учетом оборудования провайдера

IP-адрес шлюза провайдера «Provider-GW» 198.51.100.1, коммутатор провайдера «Provider-SW» пропускает через себя трафик любых VLAN.

Команда ping успешно проходит между коммутатором DSW1 и Provider-GW.

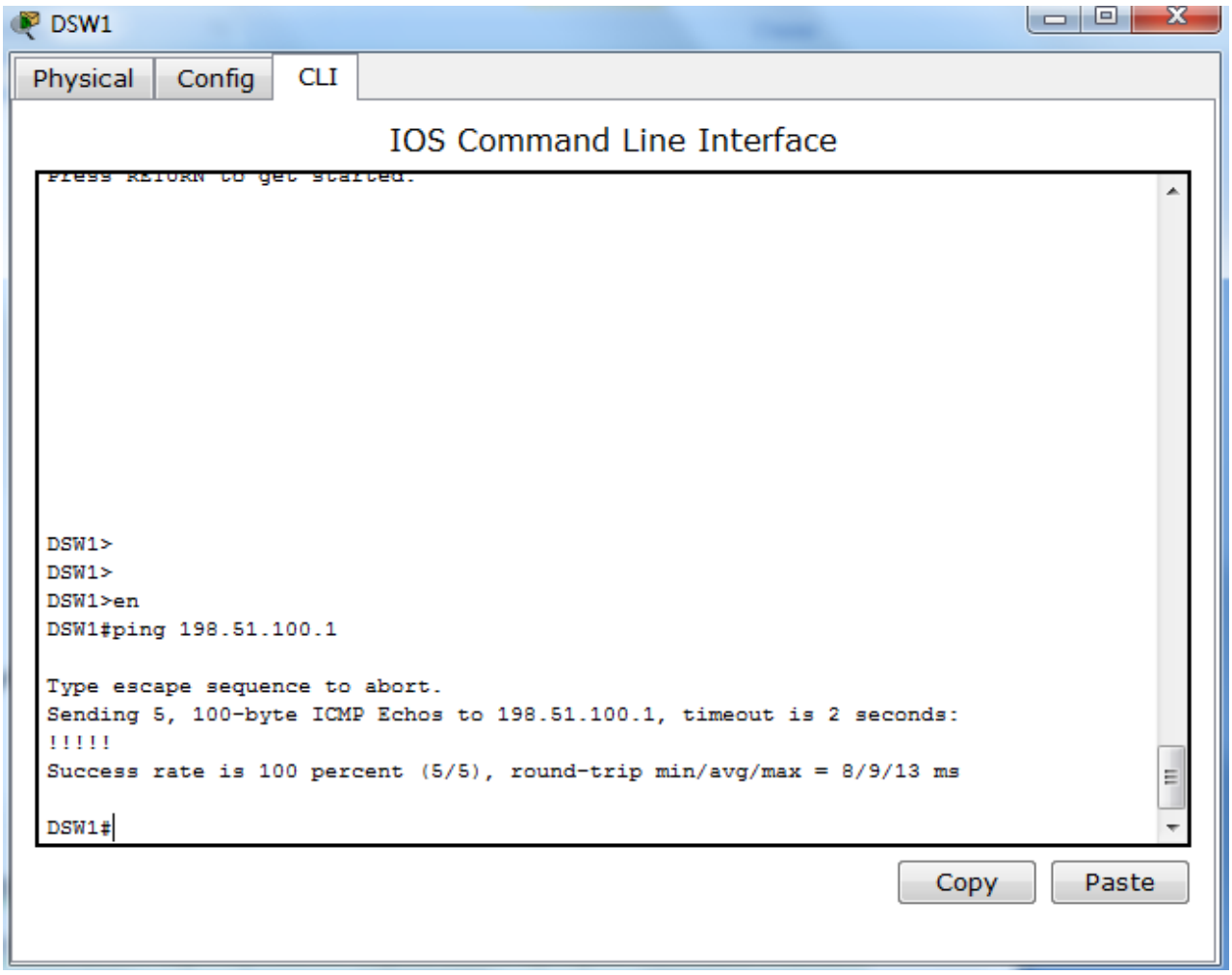


Рисунок 3.6 – Связь с оборудованием провайдера

3.5 Агрегирование каналов

Для увеличения пропускной способности между коммутаторами DSW2 и ASW2 и DSW1 и DSW2 необходимо применить агрегирование каналов.

На данный момент они соединены каналом в 1 Гбит/с, однако при критических нагрузках этого может не хватить. Поэтому следует увеличить пропускную способность на 200 Мбит/с.

/* Агрегирование каналов на DSW2 */

#configure terminal

#interface range fastEthernet 0/23-24

#switchport mode trunk

#switchport trunk allowed vlan 2,3

#channel-group 1 mode on

#interface GigabitEthernet 1/2

channel-group 1 mode on

/* Агрегирование каналов на ASW2 */

#configure terminal

#interface range fastEthernet 0/23-24

#switchport mode trunk

#switchport trunk allowed vlan 2,3

#channel-group 1 mode on

#interface GigabitEthernet 1/1

channel-group 1 mode on

/* Агрегирование каналов на DSW1 */

#configure terminal

#interface range fastEthernet 0/10-11

#switchport mode trunk

#switchport trunk allowed vlan 2,3

#channel-group 2 mode on

#interface GigabitEthernet 0/1

channel-group 2 mode on

/* Агрегирование каналов на DSW2 */

#configure terminal

#interface range fastEthernet 0/10-11

#switchport mode trunk

#switchport trunk allowed vlan 2,3

#channel-group 2 mode on

#interface GigabitEthernet 1/1

channel-group 2 mode on

4 БЕЗОПАСНОСТЬ ЖИЗНИДЕЯТЕЛЬНОСТИ

4.1 Анализ условий труда оператора

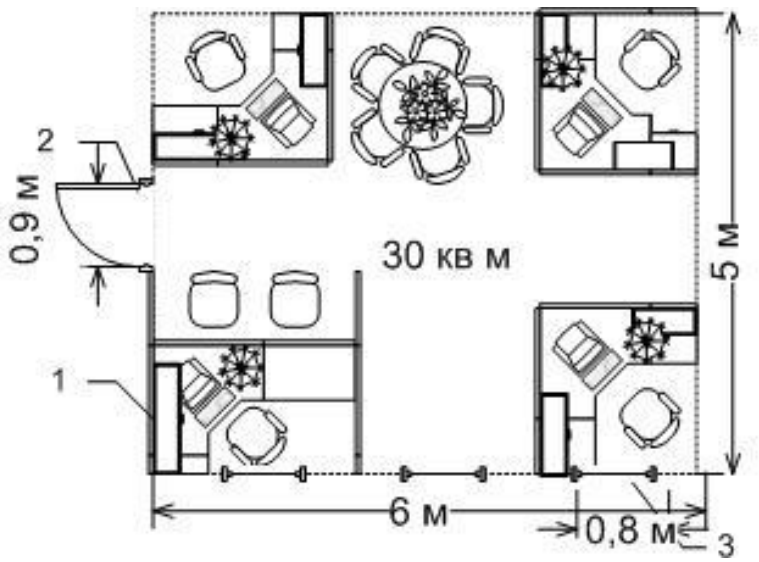
Целью дипломной работы является разработка локальной сети компании с расширенными функциональными возможностями. Благодаря использованию технологии удаленного доступа, в офисе компании будут находиться лишь 2 IT специалиста, 1 логист и координатор компании, все остальные сотрудники имеют возможность вести работу в удобном для себя месте.

Количество работников – 4 человека. Установленное оборудование представляет собой четыре компьютера, один из которых выступает в роли сервера, объединенных в локальную сеть. Соединение осуществлено с помощью экранированной медной витой пары (сетевой кабель).

График работы – полная занятость. Рабочий день составляет 8 часов в сутки, пять дней в неделю. Рабочий день начинается в 8:00, заканчивается в 17:00, перерыв на обед с 12:00 до 13:00.

Для более полного и подробного анализа условий труда необходимо учитывать следующие параметры:

- площадь помещения составляет 30 м^2 в нем 4 рабочих мест, т.е. на каждое рабочее место приходится 7,5 м^2. Можно сделать вывод, что помещение соответствует санитарным нормам проектирования предприятий, исходя из которых площадь на одно рабочее место должно быть не меньше 6м^2;
- высота потолка – 3,2 метра;
- освещение помещений - естественное. Для обеспечения освещения помещений в темное время суток и улучшения освещения при за ПК - целесообразно применение системы искусственного освещения.



1 – рабочее место, 2 – дверь, 3 – окно

Рисунок 4.1 – План офисного помещения

Весь рабочий процесс представляет из себя удаленный мониторинг и настройку корпоративной локальной сети, следовательно, категория тяжести работ в офисе Iб (ГОСТ 12.1.005-88), так как работы производятся сидя и не сопровождаются физическими напряжениями (энергозатраты до 120 кДж/час). В помещении в течение года метеоусловия находятся в следующих пределах:

- температура воздуха 21°C – 23°C;
- относительная влажность 40% - 60%;
- подвижность воздуха не более 0,1 м/с.

Что соответствует санитарным нормам для I категории тяжести работ. ГОСТ 12.1.005-88.

Для поддержания оптимальной относительной влажности и температуры воздуха необходима вентиляция помещения. Поскольку естественная вентиляция через открытые окна эффективно работает лишь до определенного значения температуры наружного воздуха, в помещении необходимо установить систему кондиционирования, подобранную в соответствии с полученными расчетами [19].

Естественное освещение офиса – боковое, одностороннее. Площадь окна 1,35 кв.м. Количество окон – 3.

4.2 Расчет искусственного освещения

Произведем анализ искусственного освещения. Для помещений, в которых предусматривается общее равномерное освещение горизонтальных поверхностей, освещение рассчитывают методом коэффициента использования светового потока.

По этому методу расчетную освещенность на горизонтальной поверхности определяют с учетом светового потока, падающего от светильников непосредственно на поверхность и отраженного света от стен, потолка и самой поверхности. Так как этот метод учитывает долю освещенности, создаваемую отраженным световым потоком, его применяют для расчета помещений, где отраженный световой поток играет существенную роль, т.е. для помещений со светлыми потолками и стенами при светильниках рассеянного, отраженного света.

Расчет освещения производится для комнаты площадью 30 м^2 , ширина которой 5 м, высота – 3,2 м. Воспользуемся методом светового потока.

Индекс помещения рассчитывается из выражения:

$$i = \frac{S}{h \cdot (A + B)_л}, \qquad (4.1)$$

где S - площадь помещения, S = 30 м ;

А – длина освещаемой поверхности, А = 6, м;

В – ширина освещаемой поверхности, В = 5, м;

$h_{св}$ – высота свеса 0 т.к. h =3,2 м;

$h_{раб}$ – высота рабочей поверхности.

$$h_р = h - h_{раб} - h_{св}, \qquad (4.2)$$

$$h_р = 3{,}2 - 1 - 0 = 2{,}2 \text{ м}$$

Тогда:

$$i = \frac{30}{2{,}2 \cdot (5 + 6)_л} = 1{,}24.$$

Исходя из данных коэффициент отражения потолка и пола по данным СНиП РК 2.04.-05.2002 $\rho_{ср}$ = 70%, т.к. потолок беленный и также стены с закрытыми белыми шторами и далее выбираем коэффициент использования светового потока, учитывая индекс помещения i = 1,24, коэффициент использования светового потока n = 0,47 [2].

Количество ламп рассчитывается по формуле:

$$N = \frac{E \cdot S \cdot z \cdot K_з}{\Phi_Л \cdot \eta \cdot n}, \qquad (4.3)$$

где E – освещенность, для IV (б) разряда работ нормируемая освещенность по таблице 3.12 [4] – 200 лк;

n – количество ламп в светильнике, n = 2;

Фл – номинальный световой поток одной лампы, используются светильники типа ПВЛМ 2х40, Фл = 3120 лм;

η – коэффициент использования светового потока. При коэффициентах отражения $\rho_{пот}$ = 70%, $\rho_{ст}$ = 50%, $\rho_{пол}$ = 30%, при индексе помещения i = 1,24, η = 47%[17];

S – освещаемая площадь, S = 30, м²;

z – коэффициент неравномерности освещения, z = 1,1.

Для помещений общественных зданий (рабочих помещений) при искусственном освещении газоразрядными лампами, исходя их СНиП РК 2.04-05-2002, коэффициент запаса $К_з$ = 1,2.

Подставляя цифровые значения, получаем:

$$N = \frac{200 \cdot 1{,}1 \cdot 30 \cdot 1{,}2}{3120 \cdot 2 \cdot 0{,}47} = 3$$

Рассчитаем расстояние между светильниками по формуле:

$$L_{A,B} = \lambda \cdot h_p \qquad (4.4)$$

Примем λ = 0,67, тогда:

L_A =0,67·2,2=1,5 м

Далее найдем расстояние до стены по следующей формуле:

$$l_{а,в} = (0{,}3 \div 0{,}5) \cdot L_{A,B} \qquad (4.5)$$

$l_а$ =0,5·1,5=0,75 м.

Расстояние L_b в нашем случае отсутствует, так как имеется всего 3 светильника. Расстояние l_b примем равным 2,5 м, так как длина светильника составляет 1,25 м, а ширина помещения равна 5 м.

При выборе осветительных приборов для административных помещений используем светильники с люминесцентными лампами. Схема размещения светильников приведена на рисунке 4.2.

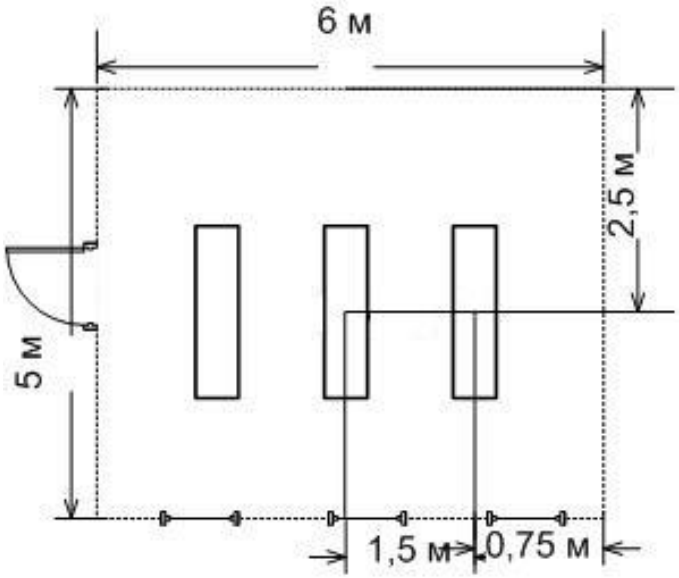


Рисунок 4.2 – Схема размещения светильников

Вывод: операторская комната имеет небольшую площадь, равную 30 м^2, поэтому как видно из расчетов, для обеспечения освещенности 200 лк достаточно 3 светильника типа ПВЛМ 2х40. Таким образом, при недостаточном естественном освещении, в вечернее время, искусственное освещение будет обеспечивать необходимую освещенность.

4.3 Расчет противопожарной безопасности

Расчет выполнен по методической литературе [7] СНиП РК 2.02.05 – 2002[8].

Электрическая пожарная сигнализация состоит приборы-извещатели, приёмный пункт пожарной сигнализации в помещении, где осуществляется круглосуточное дежурство персонала.

В качестве извещателя используется дымовой пожарный извещатель ДИП-3.

При высоте помещения 3м, площадь контролируемая одним извещателем равна 10 м^2.

Определим количество ДИП-3 по формуле (4.6):

$$M=Ц\cdot(S/S_0), \quad (4.6)$$

где Ц – Округление до ближайшего целого числа;

S – площадь помещения;

S_0 – площадь контролируемая одним ДИП-3.

$$M=Ц\cdot(36/10)=3,6.$$

Разместим в помещении 4 извещателя.

В качестве пульта извещения установим пульт «Топаз - 3 М».

С учётом того, что к пульту подключены все помещения.

Пульт «Топаз - 3 М» предназначен для контроля 10 зон извещения.

В помещении устанавливаем порошковый огнетушитель типа ОПУ-8.

Технические характеристики приведены в таблице 4.2.

Таблица 4.2 - Характеристики огнетушителя ОПУ-8

Наименования параметров	Нормы для типоразмеров огнетушителей
Масса огнетушащего вещества, кг	8
Длина порошковой струи, м; не менее.	5
Время приведения огнетушителя в действие, с; не более.	5
Время выхода порошка, с; не менее.	12
Остаток огнетушащего порошка, %; не более.	10
Температура среды доступная для использования, С.	-30 +50
Габаритные размеры: Диаметр, мм Высота, мм	 163 570
Масса заряженного огнетушителя, кг.	13,5
Площадь тушения класса В, $м^2$; не менее.	3,8
Рабочее давление, Мпа	1,2
Вместимость корпуса, г	8

Вывод: Согласно расчету выбран порошковый огнетушитель типа ОПУ-8. Масса огнетушащего вещества 8кг, габаритные размеры: диаметр 163мм, высота 570мм, длина порошковой струи 5м.

Огнетушители порошковые унифицированные типа ОПУ предназначены для тушения пожара класса А (твёрдых веществ), класса В (жидких веществ), класса С (газообразных веществ) и электроустановок до 1000 В.

Все огнетушители подвергаются периодической проверке и перезарядке.

5 БИЗНЕС-ПЛАН

5.1 Резюме

Целью данного бизнес-плана является создание удобств и преимуществ, связанные с локальной мобильностью, завоевание рынка сбыта и получение прибыли.

Основой экономической эффективности разработанной корпоративной сети компании с расширенными функциональными возможностями является высокая отказоустойчивость и длительный срок службы, простота реализации и возможного расширения, широкие функциональные возможности по передаче трафика данных, возможность работать удаленно из любой точки земного шара.

Общая сумма капитальных вложений на разработку и выполнение данного проекта составит 1768690 тенге.

Экономическая эффективность будет получена за счет экономии на электроэнергии и аренде офисного помещения и составит 4684320 тенге/год.

Конечный срок окупаемости проекта составит не более 6 месяцев.

Реализация данного бизнес-плана позволит компании занять значительную часть рынка телекоммуникационной отрасли, быстро возвратить инвестиции, позволит получить стабильный и хороший доход.

Выбранная в ходе разработки продукция Cisco будет служить намного дольше своих конкурентов и нам не придется платить за замену более быстро изнашиваемого оборудования каждые 5 лет.

5.2 Компания и отрасль

Компания будет производить удаленную продажу и техническую поддержку оборудования Cisco, которое является основным звеном телекоммуникационной отрасли казахстанской экономики.

Функциональная возможность технологии удаленного доступа, на основе которой производится работа компании, предоставляет нам следующие возможности:

Во-первых, это возможность целым отделам работать из дома. Это уменьшит расходы на аренду помещений для офисов, а так же расходы на электроэнергию.

Во-вторых, данная технология позволит стратегически важным работникам вроде руководителей и главных специалистов не отрываться от рабочего процесса, если они не могут присутствовать на рабочем месте по причине болезни, командировки, отпуска и т.д.

Иными словами, компания получает высокую мобильность своих сотрудников. К примеру:

- менеджер по продажам, находящийся на совещании с клиентом, может в любой момент воспользоваться своим ноутбуком с беспроводным доступом в Интернет и предоставить клиенту внезапно потребовавшиеся документы, или другую информацию;
- технический специалист, находясь в командировку на обслуживаемом объекте, сможет получить необходимую техническую документацию, сделать заказ на материалы, провести консультацию с коллегами;
- появляется возможность подключить к работе привлеченных специалистов из других стран;
- руководители и собственники бизнеса, имея удаленный доступ к сети предприятия, могут получать всю необходимую им оперативную

информацию, ставить задачи подчиненным и контролировать их исполнение, находясь вне офиса;

- в связи с плохим трафиком на дорогах нашего города, удаленный доступ сможет решить проблему опоздания сотрудников на работу.

В том случае если на предприятии существует развозка для сотрудников, живущих слишком далеко от места работы, отпадут затраты на бензин и заработную плату водителю.

Появляется возможность нанимать квалифицированных специалистов, имеющих проблемы с опорно-двигательным аппаратом (инвалидов). Помимо пользы рабочему процессу это принесет предприятию престиж, как месту, где уважаются права человека, и соблюдается равенство.

5.3 Описание продукции

Компания является основным в Казахстане поставщиком оборудования и продукции Cisco:

- маршрутизаторы;
- ethernet-коммутаторы;
- wi-fi точки доступа;
- платформы оптической коммутации;
- ATM-коммутаторы;
- кабельные модемы;
- серверы;
- системы видеоконференций;
- устройства сетевой безопасности;
- оборудование для IP-телефонии.

Отличительными качествами и полезностью данного оборудования являются:

- надежность: оборудование служит для пользователей на протяжении длительного срока с момента установки (до 20 лет);
- гибкость: одно и то же устройство, в зависимости от операционной системы и модуля, можно перепрограммировать, лишь набрав отдельные команды;
- взаимосвязь: все оборудование Cisco System можно связать и управлять друг другом. Это позволяет сделать сеть живым организмом, а не набором разрозненных устройств;
- интеллектуальность: все устройства содержат широкий спектр технологий, протоколов и идеологий, позволяющих расширить возможности сети.

5.4 Анализ рынка сбыта

Перспективы рынка сбыта оборудования и программного обеспечения компании в Казахстане очевидны. В круг казахстанских пользователей продуктов Cisco входят компании, лидирующие в областях своей деятельности. Показателем успеха продукции Cisco может служить перечисление ее клиентов:
- представители услуг беспроводной связи (GSM Kazakhstan/Kcell, ТОО «КаР-Тел» и ТОО «СА-Телком»/бренд Beeline, АО «ALTEL» и друге);
- представитель услуг фиксированной связи (АО «Казахтелеком»);
- представители услуг банковской сферы и другие крупные заказчики;
- госструктуры.

Основными конкурентами Cisco System по продажам телекоммуникационного оборудования на территории Казахстана можно посчитать Hewlett-Packard, Microsoft, Huawei, D-Link и Zyxel. Отличаясь своей дороговизной, один раз настроенная продукция компании Cisco служит до 20 лет бесперебойной работы, в отличие от 3-5 лет того же оборудования D-Link.

5.5 Менеджмент

По организационно-правовому статусу компания будет являться товариществом с ограниченной ответственностью, во главе которого будет генеральный директор компании - собственником данного ТОО. Также в число сотрудников компании будут входить:

- финансовый директор, ведущий все финансовые дела компании, с целью получения высокого дохода и избежание убытка для компании;
- HR специалист, проводящий рекрутинг работников компании;
- 2 советника по ротации телекоммуникационного оборудования, которые ведут связь с иностранными специалистами, следят за последними изменениями на рынке телекоммуникационного оборудования;
- 3 логиста, организовывающие рациональный процесс продвижения продукции от поставщиков к потребителям;
- 4 IT специалиста, ответственные за бесперебойную работу оборудования компании, производящие консультацию и настройку оборудования клиентов;
- 3 бухгалтера, ведущие все денежные отчеты компании;
- 4 менеджера по работе с клиентами, помогающие заказчикам с выбором оборудования и консультирующие по всем интересующим вопросам;
- 2 маркетолога, ответственные за рекламу и стимулирование спроса среди потребителей;
- переводчик компании;
- координатор, являющийся связующим среди всех сотрудников;
- нотариус, ведущий все юридические дела компании.

Общее число работников компании 24 человека.

Как уже описывалось ранее, благодаря использованию технологии удаленного доступа, в офисе компании будут находиться лишь 2 IT специалиста, 1 логист и координатор компании, все остальные сотрудники имеют возможность вести работу в удобном для себя месте.

5.6 Стратегия маркетинга

Продвижение услуг и продукции компании будет производиться в основном с помощью WEB сайта компании.

Вот уже 20 лет Cisco System является ведущим мировым поставщиком межсетевого и телекоммуникационного оборудования и программного обеспечения. Имея большую популярность и хорошее мнение среди пользователей продукции, Cisco зарекомендовала себя как надежный товар и не нуждается в большой рекламе, но для продвижения популярности компании и расширения круга потребителей будет производиться реклама в СМИ.

5.7 Финансовый план

В век информационных технологий локальные сети на предприятиях стали само собой разумеющимися и получили распространение в бизнесе любого масштаба и любого рода деятельности. Для расчета финансового плана в рамках дипломной работы остановимся на условностях, так как мы не знаем данные о годовой прибыли и численности штата.

5.7.1 Расчет инвестиционных затрат

Общие капитальные вложения [9].

$$\sum К = Ко + Кн + Км + Ктр, \qquad (5.1)$$

где Ко – капитальные вложения на приобретение оборудования;

Кн – капитальные вложения на настройку;

Км – капитальные вложения на монтажные работы;

Ктр – капитальные вложения на транспортные расходы(5% от стоимости оборудования).

Таблица 5.1 – Капитальные вложения на приобретение оборудования

Наименование оборудования	Количество единиц	Цена за единицу оборудования	Сумма в тенге
Коммутатор Cisco Catalyst 3560-24PS	1	425000	425000
Коммутатор Cisco Catalyst 2960-24TT-L	5	170000	850000
File-server	1	110000	110000
VPN-server	1	110000	111000
Кабель UTP cat 5e	1200	19	22800
Итог			1517800

Итого 1517800 тенге.

Капитальные вложения на транспортные расходы будут составлять 5% от стоимости оборудования. Таким образом:

Ктр=75890 тг.

Капитальные вложения на настройку оборудования будут высчитываться по среднерыночным ставкам на определенный вариант конфигурации оборудования.

Таблица 5.2 – Капитальные вложения на настройку оборудования

Наименование оборудования	Количество	Тариф на услугу, тенге	Сумма в тенге
Коммутатор Cisco Catalyst 3560-24PS	1	25000	25000
Коммутатор Cisco Catalyst 2960-24TT-L	5	20000	100000
File-server	1	10000	10000
VPN-server	1	20000	20000
Итог			155000

Кн=155000 тенге.

Капитальные вложения на монтажные работы.

За стоимость монтажных работ будет взята среднерыночная цена в 20000 тенге.

Км=20000 тенге.

Таблица 5.3 – Суммы вложений

Тип вложений	Стоимость в тенге
Ко	1517800
Кн	155000
Км	20000
Ктр	75890
Итого, ∑К	1768690

5.7.2 Расчет доходов

Поскольку мы не знаем данные о годовой прибыли и численности штата, расчет доходов будет производиться условно [1].

Единственным оборудованием, которое будет приносить условные доходы, которые мы сможем посчитать, является VPN-сервер, обеспечивающий технологию удаленного доступа.

Условный доход предприятию будет приносить экономия на аренде помещений и затрат на электроэнергию, входящих в эксплуатационные расходы [4].

$$\Delta Э = \Delta Э1 + \Delta Э2, \qquad (5.2)$$

где ΔЭ1 – экономия на аренде помещений;
ΔЭ2 – экономия на электроэнергии.

Мощности VPN-сервера хватит на подключение 30 удаленных пользователей. Или 30 рабочих мест.

Рассчитаем экономию за аренду помещений.

По европейским стандартам на 1 человека должно приходиться 2,5 кв. м. рабочего пространства. Средняя стоимость аренды 1 кв. м офисного помещения в Алматы – 4600 тенге/мес.

В итоге за месяц на одной только аренде помещения мы экономим

ΔЭ1 = 30*2,5*4600 = 345000 тенге/мес.

Рассчитаем экономию на электроэнергии.

Один компьютер в сутки потребляет в среднем 0,45 кВт/час. Продолжительность рабочего дня 8 часов (160 часов в месяц). Средняя стоимость 1 киловатта электроэнергии – 21 тг.

Следовательно, месячная экономия на электроэнергии составляет

ΔЭ2 = 0,45*30*160*21 = 45360 тенге/мес.

Электроэнергией, потребляемой принтерами, телефонами можно пренебречь.

В сумме экономия составит

ΔЭ = ΔЭ1 + ΔЭ2 = 390360 тенге/мес или ΔЭ = (ΔЭ1 + ΔЭ2)*12 = 4684320 тенге/год.

5.7.3 Расчет показателей экономической эффективности

Коэффициент общей экономической эффективности капитальных вложений с учетом корпоративного подоходного налога:

$$E = П/К, \qquad (5.3)$$

где П – чистая прибыль;

К – капитальные вложения.

Нашей чистой прибылью является рассчитанная ранее экономия ΔЭ. Следовательно E = ΔЭ/К.

E = 4684320/1768690 = 2,65

Срок окупаемости капитальных вложений:

$T = 1/E$.

$T = 1/2,65 = 0,38$ лет

Иными словами, капитальные вложения окупят себя примерно через 5 месяцев.

Отдельно стоит сказать о самом оборудовании Cisco.

Стоимость такого оборудования примерно в 2 раза превышает стоимость продукции ее конкурентов, более распространенных на территории Казахстана (D-Link, Zyxel и т.д.). Однако один раз настроенная Cisco-сеть будет служить до 20 лет, против 3-5 лет у того же D-Link.

ЗАКЛЮЧЕНИЕ

В результате выполнения дипломного проекта, была разработана корпоративная сеть Fast Ethernet с удаленным доступом. Сеть построена на оборудовании Cisco, также выполненная полная настройка необходимых компонентов сети. Техническое задание проекта полностью выполнено.

Во второй главе было рассмотрено основное оборудование сети, составлены планы сети, упрощающие настройку, а так же логическая топология.

Третья глава посвящена настройке сети командами Cisco IOS, показана среда моделирования и результаты настройки.

В четвертой главе были рассмотрены вопросы охраны труда, а именно: анализ условий труда, выявление опасных и вредных производственных факторов, анализ существующего искусственного освещения и расчет системы кондиционирования помещения в котором будет проходить рабочий процесс.

В пятой главе произведен расчет себестоимости проекта, а также экономический эффект от внедрения новой системы. Рассчитанный срок окупаемости составит 5 месяцев. Выгоду от внедрения новой системы можно оценить по следующим критериям:

- высокое качество оборудования Cisco;
- простота внедрения;
- отказоустойчивость сети;
- возможность изменения конфигурации;
- продолжительность срока службы составит до 20 лет.

СПИСОК ЛИТЕРАТУРЫ

1. Базылов Б.К. Методические указания для экономической части выпускной работы. – Алматы.: АИЭС, 2009. – 18 с.

2. Баранов В.Н. Применение микроконтроллеров AVR. Схемы, алгоритмы, программы – М.: Додэка, 2004. – 287 с.

3. Белов А.В. Разработка устройств на микроконтроллерах AVR. – М.: Наука и Техника, 2012. – 530 с.

4. Ворст И., Ревенлоу П. Экономика фирмы. – М.: Высшая шк.,1994. – 215 с.

5. Голубцов М.С., Кириченкова А.В. Микроконтроллеры AVR: от простого к сложному. – М.: СОЛОН–Пресс, 2006. – 304с

6. Грязнова А.Г., Юданова А.Ю. Микроэкономика: практический подход. – М.: Финансы и кредит, 2007. – 653 с.

7. Дюсебаев М.К. Безопасность жизнедеятельности: методические указания к выполнению раздела дипломных проектов. – Алматы.: АИЭС, 2003. – 27 с.

8. Евстифеев А.В. Микроконтроллеры AVR семейства Mega. – М.: Додэка, 2008. – 558 с.

9. Иващенко Н.П. Экономика фирмы: Учебник. – М.: Инфра-М, - 1999. – 196 с.

10. Князевский Б.А. Охрана труда. – М.: Высшая школа, 2002. – 365 с.

11. Кукин П.П, Лапин В.Л. Безопасность жизнедеятельности. Безопасность технологических процессов и производств. – М.: Высшая школа, - 2007. – 250 с.

12. Манн С., Крелл М. Linux. Администрирование сетей TCP/IP: Пер. с англ. – М.: Бином-Пресс, 2008. – 672 с.

13. Одом У. Официальное руководство по подготовке к сертификационным экзаменам CCNA ICND2: Пер. с англ. – М.: Вильямс, 2009. – 736 с.

14. Олифер В.Г., Олифер Н.А. Принципы, технологии, протоколы. Учебник для вузов: С.-Пб.; Энергоатомиздат, 2010. – 944 с.

15. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Информатика. Компьютеры, 2003. – 1106с.
16. Таненбаум Э. Компьютерные сети. – СПБ.: Информатика. Компьютеры, 2003. – 992с.
17. Хилл Б. Полный справочник по Cisco: Пер. с англ. – М.: Вильямс, 2004. – 1068 с.
18. Хакимжанов Т.Е. Безопасность жизнедеятельности. Расчет аспирационных систем. – А.: АИЭС, 2002. – 29 с.
19. Шантарина В.Д. Безопасность жизнедеятельности и промышленная безопасность. – Тюмень.: ТюмГНГУ, 2001. – 283 с.
20. Шпак Ю.А. Программирование на языке С для AVR и PIC микроконтроллеров. – М.: МК-Пресс, 2011. – 546 с.